V. Cryptomonnaies : au-delà du phénomène de mode

Moins de dix ans après leur apparition, les cryptomonnaies[1] sont sorties de l'ombre, suscitant un vif intérêt de la part des entreprises et des particuliers, ainsi que des banques centrales – entre autres autorités. Les cryptomonnaies attirent l'attention parce qu'elle promettent de remplacer la confiance dans des institutions établies de longue date, comme les banques commerciales et les banques centrales, par un nouveau système, intégralement décentralisé, fondé sur la « chaîne de blocs » et la technologie de registre distribué (*related distributed ledger technology*, DLT) qui lui est liée.

Le présent chapitre se propose d'évaluer la capacité des cryptomonnaies à jouer un rôle quelconque en tant que monnaie : au-delà de l'engouement qu'elles suscitent, quels types de problèmes économiques peuvent-elles résoudre dans leur forme actuelle – si tant est qu'elles puissent en résoudre aucun ? Le chapitre s'ouvre sur un rappel historique. Nombre d'épisodes passés d'instabilité monétaire et d'échec d'une monnaie témoignent de l'importance que revêtent les mécanismes institutionnels présidant à l'offre de monnaie. Les auteurs montrent qu'au fondement d'une monnaie solide réside toujours la confiance dans la stabilité de sa valeur. L'essence même d'une monnaie – servir d'instrument de coordination facilitant les transactions – exige qu'elle puisse être déployée à l'échelle de l'économie et que son offre soit élastique, pour s'adapter aux fluctuations de la demande. Des mécanismes institutionnels particuliers sont donc nécessaires, d'où l'apparition des banques centrales actuelles, indépendantes et tenues de rendre des comptes.

Le chapitre se poursuit par une introduction aux cryptomonnaies et une analyse des limites économiques propres à la confiance décentralisée qu'elles impliquent. Pour que celle-ci soit durable, les utilisateurs de bonne foi doivent maîtriser l'essentiel de la puissance de calcul et chacun d'entre eux doit vérifier l'historique des transactions ; en outre, l'offre de cryptomonnaie doit être prédéfinie par son protocole. La confiance peut disparaître à tout moment du fait de la fragilité du consensus décentralisé régissant l'enregistrement des transactions. Cela ne remet pas seulement en question l'irrévocabilité des paiements individuels, mais signifie également qu'une cryptomonnaie peut simplement s'arrêter de fonctionner, entraînant alors une perte totale de valeur. En outre, même si la confiance prévaut, la technologie en question se caractérise par une piètre efficacité et une forte consommation d'énergie. Les cryptomonnaies ne peuvent pas répondre à l'ampleur de la demande de transactions, sont sujettes à saturation et voient leur valeur fluctuer fortement. Globalement, la technologie décentralisée des cryptomonnaies, quelque sophistiquée qu'elle soit, constitue un piètre substitut à des institutions solides garantes de la monnaie.

Cependant, la technologie sous-jacente pourrait servir à d'autres applications, comme la simplification des processus administratifs pour le règlement des transactions financières. Cela reste encore à prouver néanmoins. Les cryptomonnaies soulevant bon nombre de questions, le chapitre se termine par un exposé des réponses possibles en termes de politiques publiques, dont la réglementation des usages privés de la technologie, les mesures à prendre pour prévenir les abus, et la délicate question de l'émission de monnaies numériques par les banques centrales elles-mêmes.

Mise en perspective de l'essor des cryptomonnaies

Un bon moyen de déterminer si une nouvelle technologie peut constituer un ajout vraiment utile à la panoplie monétaire existante est de prendre du recul et de revoir les fonctions fondamentales de la monnaie dans une économie, et ce que l'Histoire nous enseigne en termes de tentatives infructueuses de création de nouvelles monnaies privées. On peut ensuite se demander si une monnaie fondée sur cette nouvelle technologie peut améliorer de quelque manière que soit la panoplie monétaire actuelle[2].

Une brève histoire de la monnaie

La monnaie joue un rôle essentiel de facilitation des échanges. Avant son avènement voici plusieurs millénaires, l'échange de biens se fondait essentiellement sur la promesse que le destinataire rendrait ultérieurement la pareille à l'émetteur (c'est-à-dire sur un système de reconnaissance de dette)[3]. Néanmoins, les sociétés et l'activité économique se développant, il s'est avéré plus difficile de tenir le registre de reconnaissances de dette toujours plus complexes, et les risques de défaut et de règlement sont devenus source d'inquiétude. La monnaie et les institutions émettrices sont alors apparues pour faire face à cette complexité croissante et à la difficulté qu'elle posait en termes de maintien de la confiance.

La monnaie remplit trois fonctions fondamentales complémentaires. Elle est : (i) une unité de compte, à l'aune de laquelle il est possible de comparer les prix des objets que nous achetons, ainsi que la valeur des promesses que nous formulons ; (ii) un moyen d'échange, en ce que le vendeur l'accepte comme instrument de paiement, dans l'attente que quelqu'un d'autre en fera autant ; (iii) une réserve de valeur, permettant à ses utilisateurs de reporter leur pouvoir d'achat dans le temps[4].

Pour remplir ces fonctions, la monnaie doit avoir la même valeur à différents endroits et sa valeur doit rester stable dans le temps : il est beaucoup plus facile de décider de vendre un bien ou un service si l'on est sûr que la monnaie que l'on reçoit en échange a une valeur garantie en termes de pouvoir d'achat actuel et à venir. Une façon d'y parvenir est d'utiliser de pures monnaies marchandises ayant une valeur intrinsèque, comme du sel ou des céréales. Ces monnaies ne soutiennent cependant pas efficacement les échanges : elles ne sont pas toujours disponibles, sont coûteuses à produire et peu commodes à échanger ; en outre, elles peuvent être périssables[5].

Le développement de l'activité économique a nécessité la création de monnaies plus commodes, qui puissent répondre à la croissance de la demande, être efficaces pour le commerce et présenter une valeur stable. Néanmoins, entretenir la confiance dans les mécanismes institutionnels présidant à l'offre de monnaie a constitué le défi le plus difficile à relever. À travers le monde, en différents points et à différents moments, l'émission de la monnaie a commencé à relever d'autorités centralisées. Dans les temps anciens, la valeur d'une pièce servant à des transactions était attestée par un sceau souverain. Plus tard, les lettres de change faisant l'objet d'une intermédiation bancaire ont été conçues pour limiter les coûts et les risques liés au fait de se déplacer avec d'importantes sommes en espèces[6].

Néanmoins, l'expérience historique atteste également d'un compromis sous-jacent, car les monnaies jouissant d'une offre flexible peuvent aussi être dévaluées facilement[7]. Du point de vue historique, les longs épisodes de stabilité monétaire constituent des exceptions bien plus que la norme. En fait, la confiance a si souvent

fait défaut que l'Histoire abonde de monnaies disparues. Ce type de monnaies fait l'objet de collections dans de nombreux musées à travers le monde – c'est par exemple le cas du British Museum à Londres. Pierres, coquillages, tabac, pièces et morceaux de papier en tous genres et autres objets qui ne sont plus échangeables y sont présentés. Certaines monnaies ont été victimes du développement de l'activité économique et commerciale, devenant impropres à une utilisation à grande échelle. D'autres ont été abandonnées lorsque l'ordre politique qui les étayait s'est affaibli ou effondré. Et d'autres encore ont pâti d'une érosion de la confiance dans la stabilité de leur valeur.

La monnaie, ainsi que le montre l'Histoire, peut être fragile, que son offre passe par des moyens privés, soit assurée de manière concurrentielle ou soit le fait d'un émetteur souverain qui en détient le monopole. La qualité de la monnaie émise par les banques dépend des actifs qui l'étayent. Les banques ont pour but de transformer les risques ; par conséquent, dans certains scénarios extrêmes, la confiance dans une monnaie émise de manière privée peut disparaître du jour au lendemain. Les mécanismes garantis par l'État, dans lesquels la mission de préservation de la confiance dans l'instrument est centralisée, n'ont pas toujours bien fonctionné non plus, loin s'en faut : un exemple d'abus célèbre est la dévaluation compétitive des pièces émises par les princes allemands au début du XVIIème siècle, connue sous le nom de *Kipper- und Wipperzeit* (signifiant qu'une partie du métal des pièces était « rognée »)[8]. De nombreux autres exemples pourraient être cités comme, aujourd'hui, ceux du Venezuela ou du Zimbabwe. Éviter les abus par les émetteurs souverains a donc constitué un enjeu clé de la conception des mécanismes monétaires.

La recherche d'un cadre institutionnel solide soutenant la confiance dans la monnaie a finalement abouti à la création des banques centrales telles qu'on les connaît aujourd'hui. Dans un premier temps ont été établies des banques publiques agréées dans les cités-États européennes entre 1400 et 1600. Elles avaient pour but d'améliorer les échanges commerciaux en fournissant un moyen de paiement efficace et de qualité, et en centralisant un certain nombre d'opérations de compensation et de règlement. Ces banques, établies dans des carrefours d'échanges tels que Amsterdam, Barcelone, Gènes, Hambourg ou bien Venise, ont joué un rôle essentiel dans le dynamisme du commerce international et de l'activité économique plus généralement[9]. Au fil du temps, nombre de ces banques agréées ont fini par fonctionner à la manière des banques centrales actuelles. Les banques centrales officielles que nous connaissons aujourd'hui sont elles aussi souvent apparues à l'issue d'expériences malheureuses avec des monnaies décentralisées. Ainsi, l'échec des « wildcat banks » aux États-Unis a finalement abouti à la création du Système de Réserve fédérale.

Le système monétaire et de paiement actuel

À l'ère moderne, le système qui a fait ses preuves dans l'instauration d'une confiance résiliente est celui des banques centrales indépendantes. Il passe par l'établissement d'objectifs (en matière de politique monétaire et de stabilité financière) ; par une indépendance opérationnelle, administrative ainsi qu'au plan des instruments utilisés ; et par le principe de responsabilité démocratique, afin de garantir un soutien et une légitimité politiques suffisamment larges. Les banques centrales indépendantes sont largement parvenues à préserver l'intérêt économique et politique de la société à disposer d'une monnaie stable[10]. Dans cette configuration, la monnaie peut être précisément définie comme une « convention sociale

indispensable, soutenue par une institution responsable au sein de l'État qui jouit de la confiance du public »[11].

Dans la quasi-totalité des économies actuelles, l'offre de monnaie est le fait d'un partenariat public-privé entre la banque centrale et les banques privées, la première se situant au cœur du système. Les dépôts bancaires électroniques constituent le principal moyen de paiement entre les utilisateurs finaux, tandis que les réserves auprès de la banque centrale servent de moyen de paiement entre banques. Dans ce dispositif à deux niveaux, la confiance est produite par des banques centrales indépendantes et tenues de rendre des comptes, qui soutiennent les réserves par leurs détentions d'actifs et leurs règles opérationnelles. La confiance dans les dépôts bancaires émane, quant à elle, de différents facteurs, dont la réglementation, la supervision et les dispositifs de garantie des dépôts, qui pour beaucoup relèvent de l'État.

Dans le cadre de leur mandat consistant à assurer la stabilité de la monnaie en tant qu'unité de compte et moyen de paiement, les banques centrales jouent un rôle actif dans la supervision, la surveillance et, dans certains cas, l'offre, d'infrastructures de paiement pour leur monnaie. Les banques centrales ont notamment pour rôle de garantir le bon fonctionnement du système de paiement et de veiller à ce que l'offre de réserves réponde correctement à l'évolution de la demande, notamment de manière intra-journalière – c'est-à-dire, d'assurer une offre élastique de la monnaie[12].

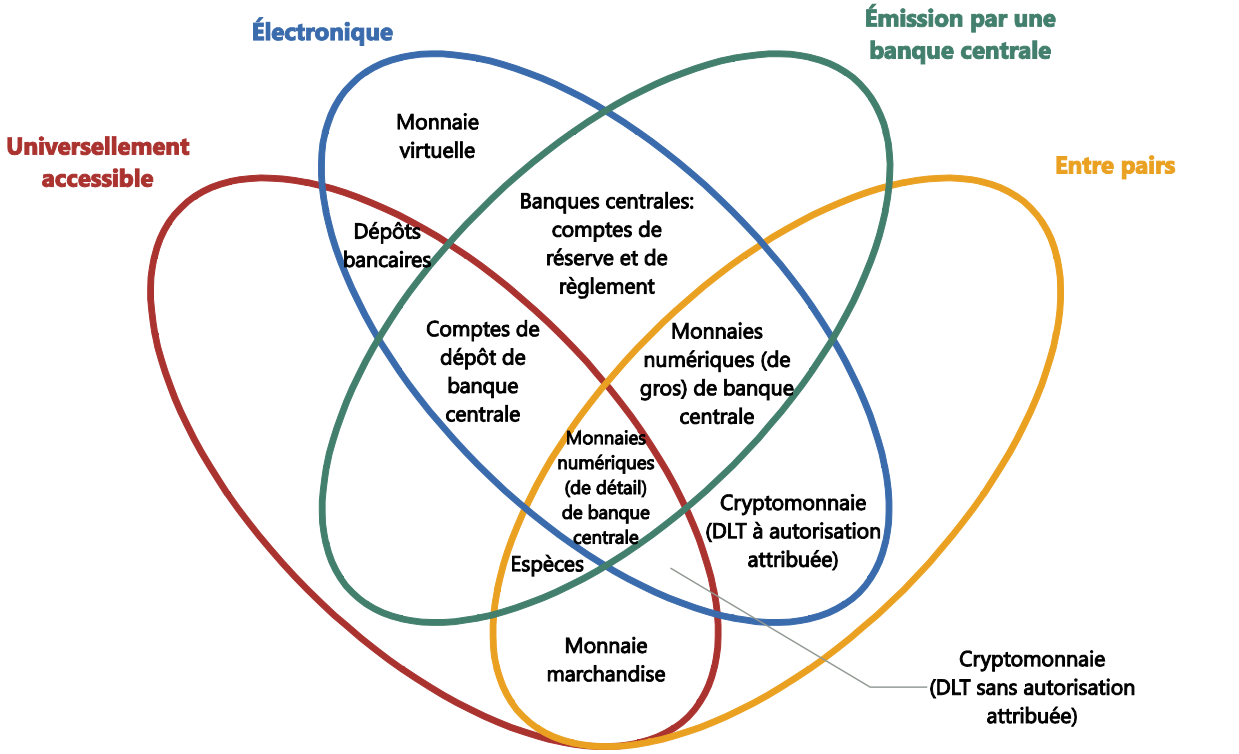
Grâce au rôle actif des banques centrales, les systèmes de paiement, dans leur diversité, sont aujourd'hui devenus sûrs, efficaces en termes de coûts, extensibles et à même de garantir qu'un paiement, une fois effectué, est irrévocable.

Ces systèmes de paiement sûrs et efficaces en termes de coûts peuvent traiter d'importants volumes de transactions et s'adapter à une croissance rapide de l'activité de manière peu onéreuse et sans abus ou presque. Le caractère extensible des systèmes de paiement contribue largement à leur sûreté et à leur efficacité en termes de coûts. Dans les économies complexes d'aujourd'hui, le volume de paiements est élevé, représentant plusieurs fois le PIB. Pour autant, l'augmentation de l'utilisation de l'instrument ne conduit pas à une augmentation proportionnelle des coûts. Il s'agit d'un point important car l'une des caractéristiques essentielles d'une bonne monnaie et d'un bon système de paiement est l'étendue de son utilisation tant par les acheteurs que par les vendeurs : plus il existe d'utilisateurs d'un système de paiement en particulier, plus un individu est incité à y recourir lui-même.

Les utilisateurs ne doivent pas seulement avoir confiance dans la monnaie elle-même, ils doivent également pouvoir compter sur une exécution rapide et sans heurt des paiements. Il est donc souhaitable que l'exécution des paiements soit assurée (on parle d' « irrévocabilité » des paiements), tout comme, en conséquence, la capacité de contester toute transaction qui aurait été mal exécutée. L'irrévocabilité nécessite que le système soit largement exempt de fraudes et de risques opérationnels, tant au plan des transactions individuelles qu'à celui du système dans son ensemble. Une solide supervision, de même que la responsabilité endossée par les banques centrales, contribuent à assurer l'irrévocabilité des paiements et donc, la confiance dans le système.

Si la plupart des transactions passent aujourd'hui par des moyens de paiement en définitive adossés aux banques centrales, une riche panoplie de moyens de paiement publics et privés s'est, au fil du temps, développée. La « corolle des monnaies » (graphique V.1) en fournit une taxonomie détaillée.[13]

La « corolle des monnaies » : une taxonomie des monnaies Graphique V.1



Source : adapté de M. Bech et R. Garratt, « Des cryptomonnaies émises par les banques centrales ? », *Rapport trimestriel BRI*, septembre 2017.

La corolle des monnaies distingue quatre propriétés clés des monnaies : l'émetteur, la forme, le degré d'accessibilité et le mécanisme de transfert de paiement. L'émetteur peut être une banque centrale, une banque, ou bien personne en particulier, comme cela était le cas lorsque la monnaie prenait la forme d'un produit de base. La monnaie peut revêtir une forme physique (par exemple, une pièce de métal ou un billet de banque), ou numérique. Elle peut être largement accessible (c'est le cas des dépôts des banques commerciales) ou d'accès réduit (réserves des banques centrales). La dernière propriété concerne le mécanisme de transfert, qui peut être entre pairs ou passer par un intermédiaire central – comme c'est le cas pour les dépôts. La monnaie s'appuie habituellement sur l'une ou l'autre des technologies de base que sont les « jetons » ou les comptes. La monnaie fondée sur des jetons, que sont par exemple les billets de banque ou les pièces, peut être échangée entre pairs, mais cet échange nécessite que le destinataire du paiement puisse vérifier la validité de l'instrument ; dans le cas des espèces, le risque est la contrefaçon. De leur côté, les systèmes fondés sur des comptes dépendent fondamentalement de la capacité à vérifier l'identité du titulaire du compte.

Cryptomonnaies : la promesse illusoire d'une confiance décentralisée

Les cryptomonnaies tiennent-elles leur promesse ? Ou finiront-elles par trouver leur place dans des cabinets de curiosités ? Pour répondre à ces questions, il convient de

définir plus précisément ce que sont les cryptomonnaies, d'en comprendre la technologie sous-jacente et d'étudier les limites économiques qu'elles présentent.

Un nouveau pétale dans la corolle des monnaies ?

Les cryptomonnaies visent à constituer une nouvelle forme de monnaie et promettent de maintenir la confiance dans la stabilité de leur valeur au moyen d'une technologie décentralisée. Elles associent trois éléments. Premièrement, une série de règles (« protocole ») qui, sous forme de code informatique, définissent les modalités de transaction des participants. Deuxièmement, un registre comptabilisant l'historique des transactions. Troisièmement, un réseau décentralisé de participants qui mettent à jour, conservent et consultent le registre des transactions conformément aux règles du protocole. Sur cette base, les défenseurs des cryptomonnaies affirment qu'elles échappent aux motivations potentiellement fâcheuses des banques et des entités souveraines.

Dans la taxonomie de la corolle des monnaies, les cryptomonnaies associent trois caractéristiques principales. D'abord, elles sont numériques, visent à constituer un moyen de paiement commode et s'appuient sur la cryptographie pour empêcher leur contrefaçon et les transactions frauduleuses. Ensuite, bien qu'elles soient créées de manière privée, elles ne sont le passif de personne en particulier : elles ne peuvent pas être remboursées et leur valeur tient uniquement au fait que l'utilisateur s'attend à ce que d'autres utilisateurs continueront de les accepter. À cet égard, les cryptomonnaies ressemblent aux monnaies marchandises (bien qu'elles ne renferment aucune valeur intrinsèque). Enfin, elles permettent un échange numérique entre pairs.

Par rapport à d'autres monnaies numériques privées, comme les dépôts bancaires, le caractère distinctif des cryptomonnaies est l'échange numérique entre pairs. Les comptes bancaires numériques existent depuis des décennies. Les « monnaies virtuelles » émises de manière privée – comme celles utilisées dans le cadre des jeux vidéo en ligne, à l'instar de World of Warcraft – sont quant à elles apparues dix ans avant les cryptomonnaies. Pour leur part, les transferts de cryptomonnaies peuvent en principe avoir lieu dans une configuration décentralisée, sans qu'une contrepartie centrale soit nécessaire à l'exécution des échanges.

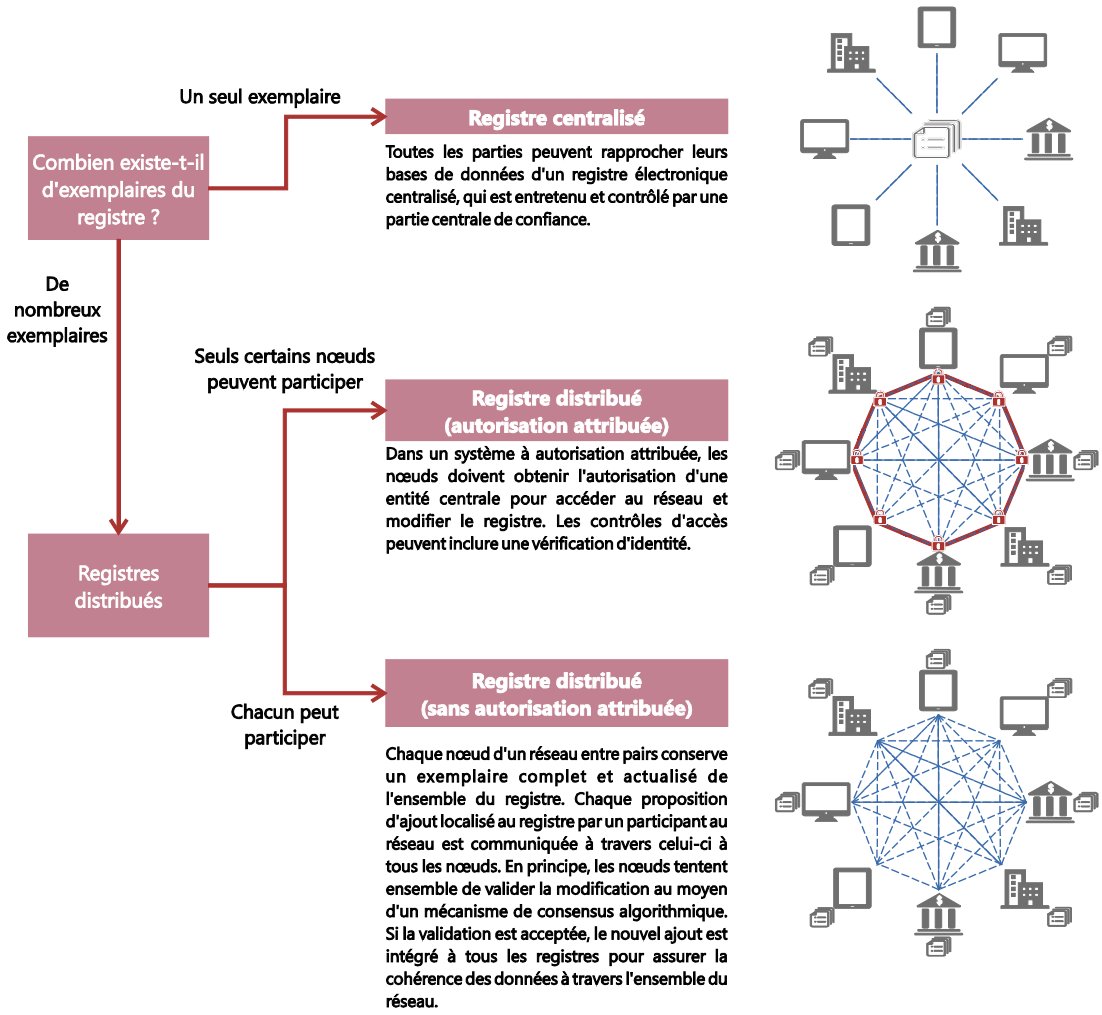
La technologie du registre distribué et son application aux cryptomonnaies

Le défi technologique à relever dans le cas de l'échange numérique entre pairs est d'éviter le « problème de la double dépense ». Toute forme numérique de monnaie est facilement reproductible et peut donc être dépensée plus d'une fois, ce qui constitue une fraude. Les informations numériques sont plus facilement reproductibles que les billets de banque physiques. Dans le cas de la monnaie numérique, résoudre le problème de la double dépense nécessite, au minimum, que quelqu'un tienne un registre de toutes les transactions. Avant l'apparition des cryptomonnaies, la seule solution consistait à confier cette tâche à un agent centralisé et à vérifier toutes les transactions.

Les cryptomonnaies surmontent le problème de la double dépense par une tenue de comptes décentralisée fondée sur un « registre distribué ». Ce registre peut se concevoir comme un fichier (à la manière d'une feuille Microsoft Excel) qui

Registre centralisé et registres décentralisés à autorisation attribuée/sans autorisation attribuée

Graphique V.2



		Monnaie électronique privée fondée sur un système fiduciaire	Cryptomonnaies émises de manière privée	
			Avec autorisation attribuée	Sans autorisation attribuée
1	Enregistrement des soldes/positions	Tenue centralisée du registre (des comptes) par des banques et autres établissements financiers	Tenue décentralisée du registre	
2	Vérification visant à éviter les doubles dépenses	Vérification d'identité	Concept de pair à pair : le registre distribué peut être consulté pour vérifier qu'une unité spécifique de compte n'a pas été déjà dépensée	
3	Traitement des transactions	Actualisation du compte par la banque	Actualisation du registre au moyen des nœuds de confiance	Actualisation du registre au moyen d'une preuve de transaction Règle consistant à suivre la chaîne la plus longue
4	Irrévocabilité/ concept de règlement	Règlement relevant uniquement de la banque centrale	Règlement dans la cryptomonnaie elle-même	Concept probabiliste d'irrévocabilité fondé sur la règle consistant à suivre la chaîne la plus longue
5	Élasticité de l'offre	Politique de la banque centrale, par exemple en matière de crédit intrajournalier	Protocole susceptible d'être modifié par les nœuds de confiance	Déterminée par le protocole
6	Mécanismes d'instauration de la confiance	Réputation des banques et des banques centrales, surveillance bancaire, prêteur en dernier ressort, lois sur les cours légaux, indépendance et responsabilité des banques centrales, vérifications AML/CFT, cybersécurité	Réputation de l'entreprise émettrice et des nœuds Nœuds de confiance, dont certains peuvent être régulés	Preuve de transaction nécessitant une majorité d'acteurs honnêtes pour effectuer les calculs

Sources : adapté de Natajaran, H., Krause, S. et Gradstein, H. (2017), « Distributed ledged technology (DLT) and blockchain », World Bank Group, *FinTech Note*, n° 1 ; BRI.

commence au moment de la distribution initiale d'une cryptomonnaie et garde ensuite la trace de toutes les transactions ultérieures. Chaque utilisateur conserve un exemplaire complet actualisé (c'est pourquoi l'on parle de registre « distribué »). Un registre distribué permet l'échange entre pairs de monnaie numérique : chaque utilisateur peut vérifier directement à l'aide de son exemplaire du registre qu'un transfert a eu lieu et qu'il n'y pas eu de tentative de double dépense[14].

Si toutes les cryptomonnaies se fondent sur un registre distribué, elles diffèrent dans la manière dont le registre est mis à jour. Deux grandes catégories se distinguent, selon leur configuration opérationnelle (graphique V.2).

La première catégorie est fondée sur une technologie de registre distribué (DLT) à autorisation attribuée. Ces cryptomonnaies sont semblables aux mécanismes de paiement traditionnels en ce sens que, pour empêcher les abus, le registre ne peut être actualisé que par des participants de confiance, souvent nommés « nœuds ». Ces nœuds sont choisis et supervisés par une autorité centrale (par exemple, l'entreprise ayant conçu la cryptomonnaie). Par conséquent, si les cryptomonnaies fondées sur des systèmes à autorisation attribuée diffèrent de la monnaie classique en termes de modalités d'enregistrement des transactions (lequel est décentralisé et non pas centralisé), elles recourent elles aussi à des garants spécifiques de la confiance dans le système[15].

Une seconde catégorie de cryptomonnaies, bien plus éloignée du modèle dominant à base institutionnelle, promettent de fonder la confiance dans un système pleinement décentralisé au moyen d'une DLT sans autorisation attribuée. Le registre des transactions ne peut être modifié que par un consensus des participants : si chacun peut participer, personne en particulier n'a de « clé » spéciale permettant de modifier le registre.

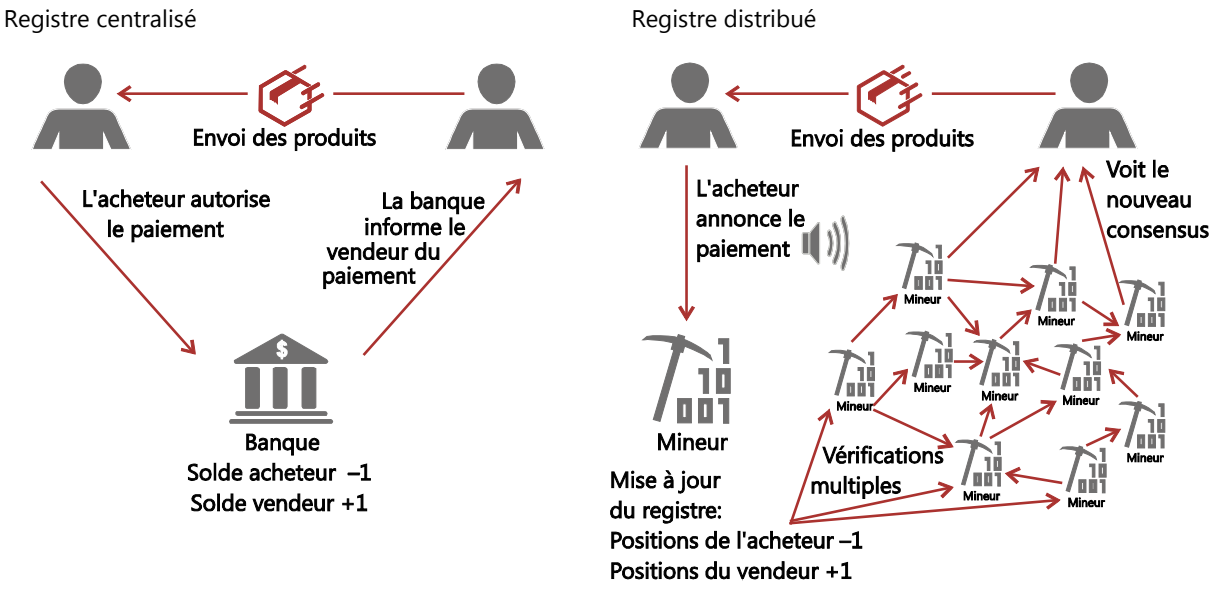
Le concept de cryptomonnaies sans autorisation attribuée a été exposé lors de la création du Bitcoin[16] dans un livre blanc rédigé par un développeur (ou un groupe de développeurs) anonyme, utilisant le pseudonyme de « Satoshi Nakamoto », et qui proposait une monnaie fondée sur un type spécifique de registre distribué : la chaîne de blocs. La chaîne de blocs est un registre distribué qui est actualisé par groupes de transactions nommés « blocs ». Les blocs sont ensuite enchaînés, au moyen de techniques cryptographiques, afin de former une chaîne de blocs. Le Bitcoin n'est qu'une des très nombreuses cryptomonnaies fondées sur ce concept[17].

Les cryptomonnaies sans autorisation attribuée fondées sur la chaîne de blocs comptent deux types d'intervenants : les « mineurs », qui tiennent le registre, et les « utilisateurs », qui souhaitent effectuer des transactions dans la cryptomonnaie. À première vue, l'idée à la base de ces cryptomonnaies est simple : au lieu d'affecter l'enregistrement des transactions de manière centralisée à une banque (graphique V.3, cadre de gauche), le registre est actualisé par un mineur et l'exemplaire actualisé est ensuite conservé par tous les utilisateurs et mineurs (graphique V.3, cadre de droite)[18].

La caractéristique principale de ces cryptomonnaies est la mise en œuvre d'une série de règles (le « protocole ») visant à faire converger les intérêts de tous les participants, de façon à créer une technologie de paiement fiable, sans agent de confiance central. D'une part, le protocole détermine l'offre de l'actif afin d'en empêcher la dévaluation ; dans le cas du Bitcoin, il prévoit que l'offre de bitcoins ne peut dépasser 21 millions d'unités. D'autre part, le protocole est conçu de telle sorte que l'ensemble des participants ait intérêt à suivre ces règles : elles créent un équilibre qui s'auto-entretient. Trois points clés sont à souligner ici.

Représentation de transactions valables dans un registre distribué/compte bancaire et dans le cadre d'une cryptomonnaie sans autorisation attribuée

Graphique V.3



Un acheteur achète un bien à un vendeur, qui, à la réception de la confirmation du paiement, procède à l'envoi du bien. Si le paiement est effectué par l'intermédiaire de comptes bancaires – c'est-à-dire d'un registre centralisé, cadre de gauche – l'acheteur envoie l'instruction de paiement à sa banque, qui actualise le solde du compte en débitant le montant payé par l'acheteur et en créditant le compte du vendeur. La banque, ensuite, confirme le paiement au vendeur. En revanche, si le paiement est effectué à l'aide d'une cryptomonnaie sans autorisation attribuée (cadre de droite), l'acheteur fait d'abord part publiquement d'une instruction de paiement indiquant que les positions de l'acheteur dans la cryptomonnaie sont réduites d'une unité, tandis que celles du vendeur sont augmentées d'une unité. Après quelques temps, un mineur intègre cette information de paiement dans un exemplaire actualisé du registre. Le registre actualisé est ensuite partagé avec d'autres mineurs et utilisateurs, chacun vérifiant que l'instruction de paiement récemment ajoutée ne constitue pas une double dépense et est autorisée par l'acheteur. Le vendeur note alors que le registre incluant l'instruction de paiement est bien celui qu'utilise habituellement le réseau de mineurs et d'acheteurs.

Source : adapté de Auer, R., « The mechanics of decentralised trust in Bitcoin and the block chain » *BIS Working Papers*, à paraître.

Premièrement, les règles entraînent un coût d'actualisation du registre. Dans la plupart des cas, ce coût est lié au fait que l'actualisation nécessite une « preuve de transaction ». Il s'agit d'une preuve mathématique qu'un certain travail de calcul a été fait, lequel nécessite un matériel coûteux et une consommation d'électricité. Comme le traitement de cette preuve de transaction prend la forme d'une extraction de nombres rares à l'aide de calculs compliqués, il est souvent désigné sous le nom de « minage »[19]. En rémunération de leurs efforts, les mineurs reçoivent des frais versés par les utilisateurs – et, lorsque le protocole le prévoit, des unités nouvellement créées de cryptomonnaie.

Deuxièmement, tous les mineurs et utilisateurs d'une cryptomonnaie vérifient toutes les actualisations du registre, ce qui conduit les mineurs à n'inclure que les transactions valables. Pour être valables, les transactions doivent provenir des détenteurs de fonds et ne doivent pas être des tentatives de double dépense. Si une actualisation de registre inclut une transaction non valable, elle est rejetée par le réseau et le mineur perd sa rémunération. La vérification de toutes les nouvelles actualisations du registre par le réseau de mineurs et d'utilisateurs est donc nécessaire pour inciter les mineurs à n'ajouter que des transactions valables[20].

Troisièmement, le protocole précise les règles permettant d'aboutir à un consensus sur l'ordre des actualisations du registre. Cela consiste généralement à

inciter chaque mineur à suivre la majorité des autres mineurs lorsqu'ils effectuent les actualisations. Une telle coordination est nécessaire, par exemple, dans les cas où des retards de communication conduisent différents mineurs à procéder à des actualisations contradictoires – par exemple, des actualisations incluant différentes séries de transactions (voir encadré V.A).

Sur la base de ces règles clés, il est coûteux – mais pas impossible – pour un individu de contrefaire une cryptomonnaie. Pour réussir à effectuer une double dépense, un faussaire devrait dépenser sa cryptomonnaie auprès d'un commerçant et produire secrètement une fausse chaîne de blocs dans laquelle cette transaction ne serait pas enregistrée. À réception de la marchandise, il communiquerait alors la fausse chaîne de blocs (procédant à une annulation de paiement). Toutefois, cette chaîne de bloc contrefaite n'apparaîtrait comme la chaîne communément acceptée que si elle était plus longue que la chaîne produite dans le même temps par le reste du réseau de mineurs. Pour réussir, une fraude à la double dépense nécessite donc une part importante de la puissance de calcul de la communauté de mineurs. À l'inverse, pour citer le livre blanc originel du Bitcoin, une cryptomonnaie peut uniquement surmonter le problème de la double dépense de manière décentralisée si « les nœuds de bonne foi contrôlent une majorité de la puissance [de calcul] »[21].

Limites économiques des cryptomonnaies sans autorisation attribuée

Les cryptomonnaies comme le Bitcoin revendiquent non seulement d'être un moyen de paiement commode fondé sur la technologie numérique, mais aussi un nouveau modèle de confiance. Cette promesse se fonde toutefois sur une série de postulats : le fait que des mineurs honnêtes contrôlent la grande majorité de la puissance de calcul, que les utilisateurs vérifient l'historique de l'ensemble des transactions et que l'offre de monnaie soit prédéterminée par un protocole. Comprendre ces postulats est important car ils soulèvent deux questions de base quant à l'utilité des cryptomonnaies. Premièrement, cette tentative compliquée de produire de la confiance se fait-elle au détriment de l'efficacité du système ? Deuxièmement, est-il vraiment et toujours possible d'instaurer la confiance ?

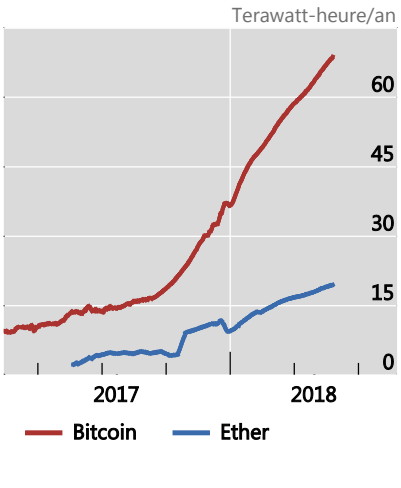
Comme le sous-entend la première question, une limite potentielle clé en termes d'efficacité tient au coût de production d'une confiance décentralisée. On s'attendrait à ce que les mineurs se concurrencent pour ajouter de nouveaux blocs au registre au moyen des preuves de transaction jusqu'à ce qu'ils n'obtiennent plus aucun bénéfice[22]. Les installations exploitées par les mineurs peuvent abriter une puissance de calcul équivalente à celle de millions d'ordinateurs personnels. Au moment où nous rédigions ce chapitre, l'utilisation totale d'électricité pour le minage de bitcoins était égale à celle de petites économies comme la Suisse, et d'autres cryptomonnaies consomment également d'abondantes quantités d'électricité (graphique V.4, cadre de gauche). Autrement dit, la quête de confiance décentralisée est vite devenue une catastrophe pour l'environnement[23].

Mais les problèmes économiques sous-jacents dépassent de loin la seule question de la consommation d'énergie. Ils sont liés à la spécificité par excellence de la monnaie : celle de promouvoir les « externalités de réseau » parmi les utilisateurs et de servir ainsi de moyen de coordination de l'activité économique. Les cryptomonnaies présentent trois lacunes en la matière : leur déploiement n'est pas pas extensible, leur valeur n'est pas stable et la confiance dans l'irrévocabilité des paiements est fragile.

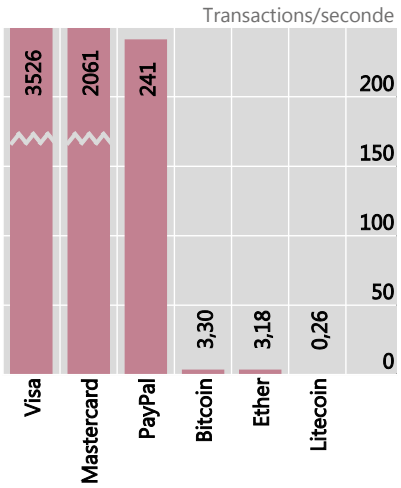
Consommation d'énergie et problèmes d'extensibilité

Graphique V.4

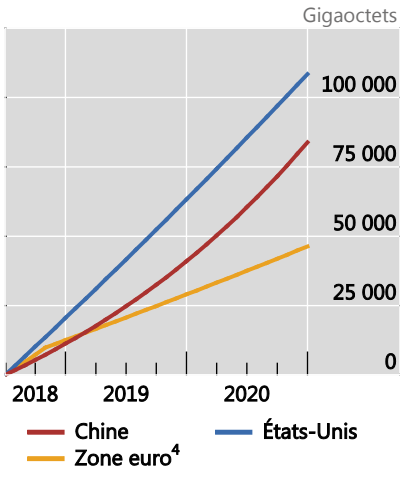
Utilisation d'énergie d'un échantillon de cryptomonnaies[1]



Nombre de transactions par seconde[2]



Taille hypothétique d'un registre de cryptomonnaie de détail à l'échelle d'une nation[3]



[1] Estimation. [2] Données de 2017. [3] La taille hypothétique de la chaîne de blocs/du registre qui est représentée sur le graphique est calculée à supposer que, à partir du 1er juillet 2018, toutes les transactions de détail non effectuées en espèces en Chine, aux États-unis ou dans la zone euro seront réalisées à l'aide d'une cryptomonnaie. Les calculs se fondent sur les informations du CPIM (2017) relatives aux transactions hors espèces, en postulant que chaque transaction ajoute 250 octets au registre. [4] BE, FR, DE, IT et NL.

Sources : www.bitinfocharts.com ; Digiconomist ; Mastercard ; PayPal ; Visa ; Comité sur les paiements et infrastructures de marché, *Statistics on payment, clearing and settlement systems in the CPMI countries*, décembre 2017 ; et calculs BRI.

Tout d'abord, les cryptomonnaies ne présentent pas le caractère extensible des monnaies souveraines. Au niveau le plus basique, celui de tenir leur promesse d'une confiance décentralisée, les cryptomonnaies requièrent de chaque utilisateur qu'il télécharge et vérifie tout l'historique des transactions, y compris les montants payés, l'émetteur du paiement et son destinataire, entre autres détails. Chaque transaction se traduisant par quelques centaines d'octets supplémentaires, le registre croît fortement au fil du temps. Ainsi, au moment où nous rédigions ce chapitre, la chaîne de blocs du Bitcoin augmentait au rythme d'environ 50 Go par an, atteignant à ce stade environ 170 Go. Par conséquent, pour que la taille du registre et le temps nécessaire à la vérification de toutes les transactions (qui augmentent avec les blocs) restent gérables, les cryptomonnaies ne peuvent pas dépasser une certaine fréquence de transactions (graphique V.4, cadre central).

Une projection hypothétique de l'utilisation des cryptomonnaies (graphique V.4, cadre de droite) montre qu''elles ne peuvent pas constituer un moyen de paiement adéquat au quotidien (graphique V.4, cadre de droite). Si les transactions numériques de détail actuellement prises en charge par les systèmes de paiement de détail nationaux des pays sélectionnés devaient être traitées au moyen de cryptomonnaies, et ce même sur la base d'hypothèses optimistes, la taille du registre augmenterait bien au-delà de la capacité de stockage d'un smartphone classique en l'espace de quelques jours, elle dépasserait la capacité de stockage d'un ordinateur individuel en quelques semaines, et celle des serveurs en quelques mois. La capacité de stockage ne constitue qu'une dimension du problème ; la capacité de traitement en est une autre : seuls des superordinateurs pourraient gérer la vérification de l'ensemble des transactions entrantes. Les volumes de communication concernés pourraient rapidement entraîner l'arrêt d'internet, l'échange de fichiers de millions d'utilisateurs atteignant un téraoctet.

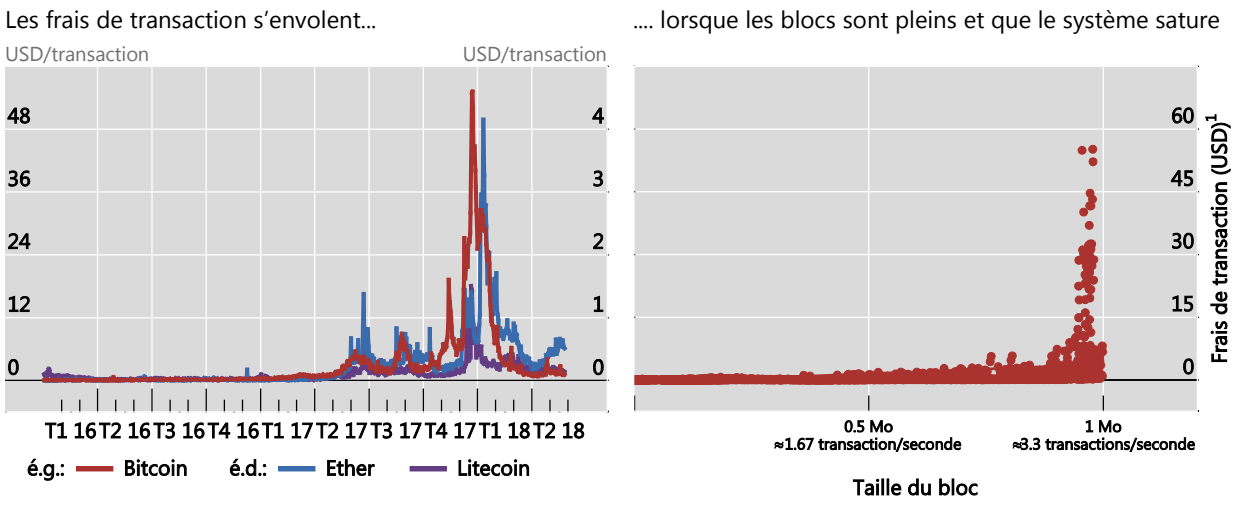
Autre difficulté liée au manque d'extensibilité des cryptomonnaies : l'actualisation du registre est sujette à saturation. Ainsi, dans le cas des cryptomonnaies fondées sur la chaîne de blocs, de nouveaux blocs ne peuvent être créés qu'à une fréquence prédéterminée, afin de limiter le nombre de transactions ajoutées au registre à quelque moment que ce soit. Lorsque le nombre de transactions entrantes est tel que les blocs nouvellement ajoutés atteignent déjà la taille maximale permise par le protocole, le système sature et de nombreuses transactions rejoignent une file d'attente. Les limites en termes de capacité signifient que les frais s'envolent dès que la demande de transactions atteint le plafond (graphique V.5). En outre, il est arrivé que les transactions demeurent en file d'attente pendant plusieurs heures, interrompant le processus de paiement. L'utilité des cryptomonnaies pour les transactions quotidiennes – l'achat d'un café, le règlement des frais d'inscription à une conférence –, sans même parler des paiements de gros, est donc limitée[24]. Par conséquent, plus les utilisateurs d'une cryptomonnaie réalisent de transactions, plus le processus de paiement devient lourd, ce qui invalide une propriété essentielle de la monnaie telle qu'on la conçoit aujourd'hui : plus elle est utilisée, plus l'incitation à l'utiliser est forte[25].

Le deuxième grand problème que posent les cryptomonnaies a trait à l'instabilité de leur valeur. De fait, aucun émetteur central n'a pour mandat de garantir la stabilité de ces monnaies. Bien gérées, les banques centrales parviennent à stabiliser la valeur intérieure d'une monnaie souveraine en ajustant l'offre de moyens de paiement à la demande de transactions. Elles procèdent à cet ajustement très fréquemment, notamment en période de tensions sur les marchés, mais aussi en temps normal.

Ce n'est pas le cas des cryptomonnaies, où le fait d'inspirer une certaine confiance dans la valeur de la monnaie nécessite que l'offre soit prédéterminée par un protocole. L'offre d'une cryptomonnaie ne peut donc pas être élastique. Par conséquent, toute fluctuation de la demande a un impact sur la valorisation. Les valorisations des cryptomonnaies sont donc extrêmement volatiles (graphique V.6, cadre de gauche). Il est peu probable que l'amélioration des protocoles ou l'ingénierie financière permettent de surmonter totalement l'instabilité intrinsèque des cryptomonnaies, comme en témoigne l'expérience du « Dai ». Conçu de façon à être

Frais de transaction au fil du temps, au regard de la fréquence des transactions

Graphique V.5



[1] Frais de transaction versés aux mineurs entre le 1er août 2010 et le 25 mai 2018, moyennes quotidiennes.

Sources : www.bitinfocharts.com ; et calculs BRI.

arrimé au dollar au taux d'un dai pour un dollar, il a touché un point bas à 0,72 dollar quelques semaines à peine après son lancement fin 2017. D'autres monnaies conçues pour conserver une valeur stable ont également fluctué très sensiblement (graphique V.6, cadre central).

Il ne s'agit pas d'une coïncidence. Assurer l'adéquation entre l'offre de moyens de paiement et la demande de transactions nécessite la présence d'une autorité centrale, généralement une banque centrale, à même d'augmenter ou de réduire son bilan. Cette autorité doit être disposée, de temps en temps, à agir à l'encontre du marché, même si elle doit ce faisant prendre des risques sur son bilan et absorber une perte. Dans un réseau décentralisé d'utilisateurs de cryptomonnaie, il n'existe pas d'agent central ayant soit l'obligation, soit intérêt à stabiliser la valeur de la monnaie : lorsque la demande de cryptomonnaie baisse, son prix baisse également.

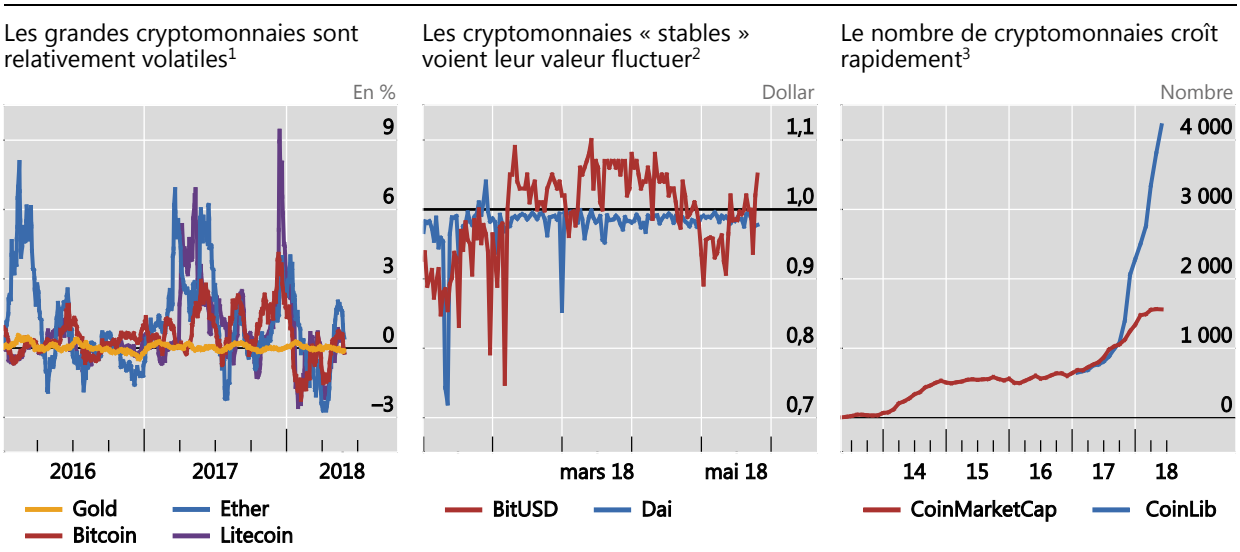
Un autre facteur contribuant à l'instabilité de valorisation est la vitesse à laquelle de nouvelles cryptomonnaie – qui tendent toutes à être interchangeables – font leur apparition. Au moment où nous rédigions ce chapitre, plusieurs milliers de ces monnaies existaient déjà ; compte tenu de leur prolifération, il est impossible d'estimer de manière fiable le nombre précis de cryptomonnaies en circulation (graphique V.6, cadre de droite). Si l'on s'en réfère aux expériences passées de la banque privée, l'émission de nombreuses nouvelles monnaies est rarement garante de stabilité.

Le troisième problème que posent les cryptomonnaies tient à la fragilité de la confiance qu'elles inspirent. Cette fragilité est elle-même due aux incertitudes qui entourent l'irrévocabilité des paiements, ainsi que la valeur des cryptomonnaies.

Dans les systèmes de paiement classiques, une fois qu'un paiement est passé par le système national de traitement des paiements puis a été comptabilisé par la banque centrale, il ne peut pas être révoqué. Les cryptomonnaies sans autorisation attribuée, au contraire, ne peuvent pas garantir l'irrévocabilité des paiements. Une

Volatilité d'un échantillon de cryptomonnaies et nombre de cryptomonnaies

Graphique V.6



[1] Moyennes mobiles sur 30 jours des rendements quotidiens. [2] Cours journalier minimum. [3] Sur la base des chiffres mensuels de deux fournisseurs. CoinMarketCap n'inclut que les cryptomonnaies dont les volumes d'échanges sur 24 heures atteignent 100 000 dollars ; CoinLib n'utilise pas de seuil.

Sources : www.bitinfocharts.com ; www.coinlib.io ; www.coinmarketcap.com ; Datastream.

raison en est que, si les utilisateurs peuvent vérifier qu'une transaction particulière est intégrée dans un registre, des versions concurrentes de ce registre peuvent exister à leur insu. Cette situation peut aboutir à des annulations de transaction, par exemple lorsque deux mineurs actualisent le registre quasi-simultanément. Une seule de ces mises à jour pouvant être conservée, l'irrévocabilité des paiements effectués dans chaque version du registre n'est qu'une probabilité.

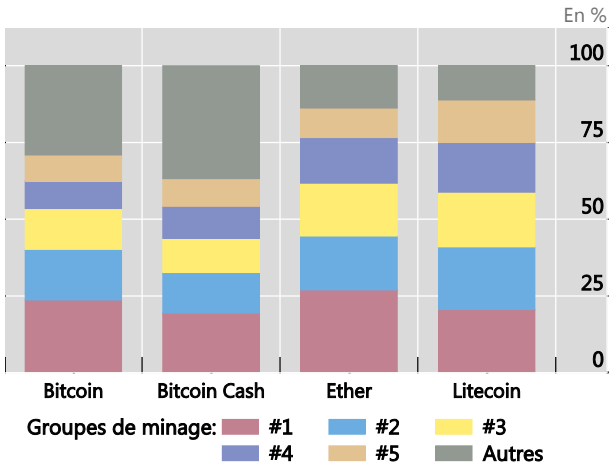
Cette absence d'irrévocabilité des paiements est d'autant plus sensible que les cryptomonnaies peuvent être manipulées par des mineurs contrôlant une vaste puissance de calcul, une hypothèse tout à fait plausible compte tenu de la concentration du minage dans un grand nombre de cas (graphique V.7, cadre de gauche). Il est impossible d'affirmer qu'une telle manipulation stratégique est en cours car le responsable ne ferait état du registre (falsifié) qu'une fois sûr du succès de sa démarche. En d'autres termes, l'irrévocabilité restera toujours incertaine. Chaque actualisation du registre d'une cryptomonnaie s'accompagne d'une preuve de transaction supplémentaire qu'un fraudeur devrait reproduire. Si la probabilité qu'un paiement soit irrévocable s'accroît avec le nombre de mises à jour ultérieures du registre, elle n'atteint jamais 100 %[26].

Non seulement la confiance dans chaque paiement est incertaine, mais en outre les bases de la confiance dans chaque cryptomonnaie sont fragiles. Ceci est dû au phénomène de bifurcation (« forking ») des registres. Il s'agit d'un processus dans lequel une partie des détenteurs d'une cryptomonnaie décident ensemble d'utiliser une nouvelle version du registre et du protocole, tandis que les autres continuent de se servir de la version originale. Ce faisant, la cryptomonnaie se scinde en deux sous-réseaux d'utilisateurs. S'il existe de nombreux exemples récents de ce phénomène, l'épisode du 11 mars 2013 est particulièrement remarquable parce que – contrairement à l'idée de créer la confiance par des moyens décentralisé – il a été résolu par une coordination centralisée des mineurs. À cette date, une actualisation

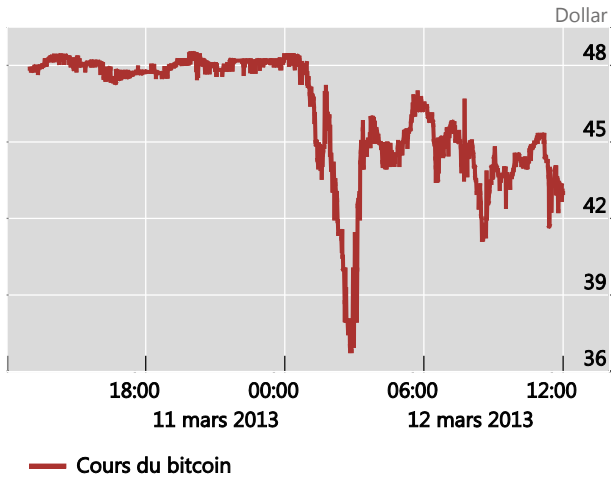
Concentration du minage et chute de la valeur du bitcoin lors d'un épisode de bifurcation

Graphique V.7

Dans toutes les cryptomonnaies, le minage est fortement concentré[1]



Chute de la valeur du bitcoin durant un épisode de bifurcation en 2013[2]



[1] Données sur les principaux groupes de minage au 28 mai 2018. [2] Évolution du cours du Bitcoin lors de l'épisode de bifurcation des 11 et 12 mars 2013.

Sources : www.btc.com ; www.cash.coin.dance ; CoinDesk ; www.etherchain.org ; www.litecoinpool.org.

erronée de logiciel a généré des incompatibilités entre une partie du réseau du Bitcoin, dont le minage se fondait sur le protocole original, et une autre partie du réseau, dont le minage se fondait sur une version mise à jour. Durant plusieurs heures, deux chaînes de blocs séparées se sont développées, et une fois que l'information s'est répandue, le cours du bitcoin a chuté de près d'un tiers (graphique V.7, cadre de droite). Cette bifurcation du registre a finalement été annulée par un effort coordonné des mineurs, qui se sont provisoirement écartés du protocole, ignorant la chaîne la plus longue. Cependant, un grand nombre de transactions ont été invalidées alors que les utilisateurs les pensaient définitives depuis plusieurs heures. Cet épisode montre la facilité avec laquelle les cryptomonnaies peuvent se scinder, conduisant à d'importantes pertes de valeur.

Ce type d'événement a ceci de plus inquiétant encore que la bifurcation du registre pourrait révéler en fait une faille fondamentale, à savoir la fragilité du consensus décentralisé procédant à l'actualisation du registre et donc, de la confiance sous-jacente dans la cryptomonnaie. L'analyse théorique (encadré V.A) laisse penser que la coordination des modalités d'actualisation du registre pourrait disparaître à tout moment, entraînant une perte totale de valeur.

Globalement, les cryptomonnaies décentralisées pâtissent d'une série de lacunes. Les principales sources d'inefficacité tiennent au degré extrême de décentralisation : instaurer la confiance requise dans un tel système consomme de grandes quantités de puissance de calcul ; le stockage décentralisé d'un registre de transaction est inefficient ; enfin, le consensus décentralisé est vulnérable. Certaines de ces failles pourraient être comblées à l'aide de nouveaux protocoles et autres innovations[27]. D'autres semblent toutefois inhérentes à ces systèmes décentralisés peu extensibles et fragiles. En définitive, l'absence d'un mécanisme institutionnel adéquat au plan national apparaît comme la principale lacune.

Au-delà de la bulle : champs d'application possibles de la technologie du registre distribué

Si les cryptomonnaies ne peuvent prétendre à être de véritables monnaies, la technologie qui les sous-tend pourrait être prometteuse dans d'autres domaines, notamment dans les services de paiement transfrontières de faible volume. Plus généralement, par rapport aux solutions technologiques centralisées classiques, la DLT peut s'avérer efficace dans des configurations de niche où l'accès décentralisé présente des bénéfices supérieurs au surcroît de coûts opérationnels liés à la tenue de multiples exemplaires du registre.

Assurément, les solutions de paiement de ce type diffèrent fondamentalement des cryptomonnaies. Un exemple récent dans le domaine des organismes à but non lucratif est le système « Building Blocks » du Programme alimentaire mondial, qui se fonde sur la chaîne de blocs pour gérer les paiements servant à l'aide alimentaire aux réfugiés syriens en Jordanie. L'unité de compte et moyen de paiement ultime du système est la monnaie souveraine : il s'agit donc d'un système de « cryptopaiement », mais pas de cryptomonnaie. Le dispositif fait en outre l'objet d'un contrôle central de la part du Programme alimentaire mondial, et ce à juste titre : une expérience initiale fondée sur le protocole Ethereum sans autorisation attribuée s'était caractérisée par des transactions lentes et coûteuses. Le système avait ensuite été repensé afin de fonctionner selon une version à autorisation attribuée du

protocole Ethereum. Cette nouvelle version a permis une réduction des coûts de transaction d'environ 98 % par rapport aux solutions bancaires alternatives[28].

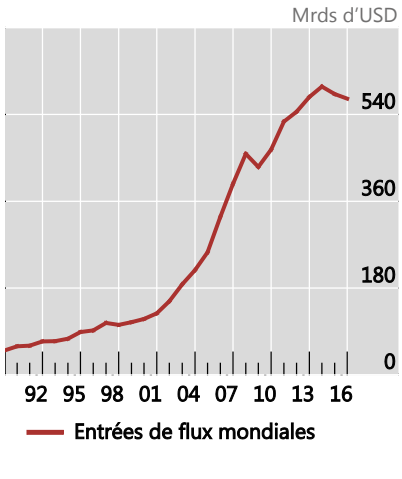
Les systèmes de cryptopaiement à autorisation attribuée pourraient aussi servir aux transferts transfrontières de faible valeur, qui jouent un rôle important dans les pays dont une grande partie de la main d'œuvre vit à l'étranger. Les flux mondiaux d'envois de fonds dépassent 540 milliards de dollars chaque année (graphique V.8, cadres de gauche et du centre). Aujourd'hui, les paiements internationaux passent par de multiples intermédiaires, ce qui se traduit par des coûts élevés (cadre de droite). Cela étant, si les systèmes de cryptopaiement constituent une solution pour répondre à ces besoins, d'autres technologies sont également envisagées et on ne sait pas à ce stade laquelle d'entre elles s'avérera la plus efficace.

Des exemples plus importants d'utilisation de la DLT associeront probablement les cryptopaiements à des codes sophistiqués à exécution automatique et à des systèmes d'autorisation de données. Aujourd'hui déjà, certains protocoles décentralisés de cryptomonnaie comme Ethereum permettent l'utilisation de contrats intelligents (« smart contracts ») qui exécutent automatiquement les flux de paiement liés aux produits dérivés. À ce stade, l'efficacité de ces produits est limitée en raison de la faible liquidité et des inefficiences intrinsèques des cryptomonnaies sans autorisation attribuée. Toutefois, la technologie sous-jacente peut être adoptée par des plateformes d'échanges agréées dans le cadre de protocoles à autorisation attribuée qui s'appuient sur la monnaie souveraine, simplifiant l'exécution du règlement. La valeur ajoutée de cette technologie proviendra probablement de la simplification des procédures administratives liées aux transactions financières complexes, comme le crédit commercial (encadré V.B). Il faut toutefois noter qu'aucune de ces applications ne nécessite l'utilisation ou la création d'une cryptomonnaie.

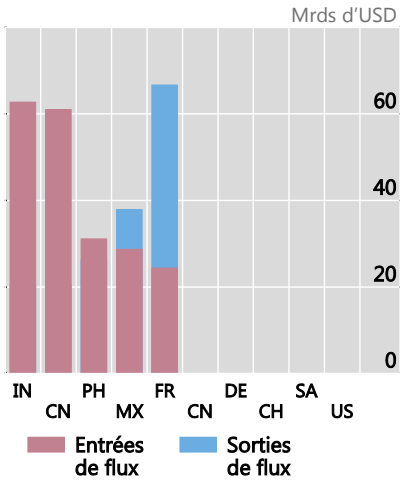
Indicateurs du volume et des coûts des envois de fonds

Graphique V.8

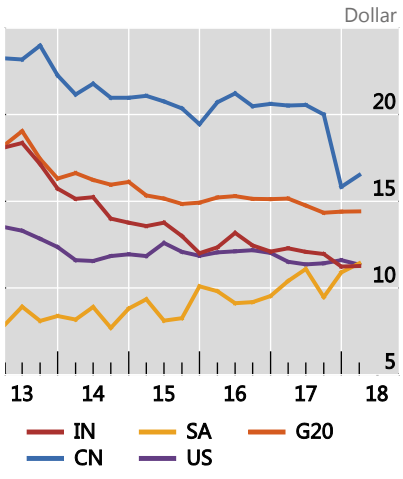
Les volumes d'envois de fonds augmentent...



... donnant lieu à de nombreux paiements de faible montant entre paires de devises souvent peu liquides...[1]



.... à des coûts moyens élevés[2]



[1] Données relatives à 2016. [2] Coût total moyen pour l'envoi de 200 dollars via l'ensemble des prestataires de transfert de fonds à l'échelle mondiale. CN et IN : coût total moyen dans le pays destinataire ; G20, SA et US : coût total moyen dans le pays émetteur.

Sources : Banque mondiale, *Remittance Prices Worldwide*, disponible en ligne : remittanceprices.worldbank.org ; Banque mondiale ; et calculs BRI.

Implications en termes de politiques publiques

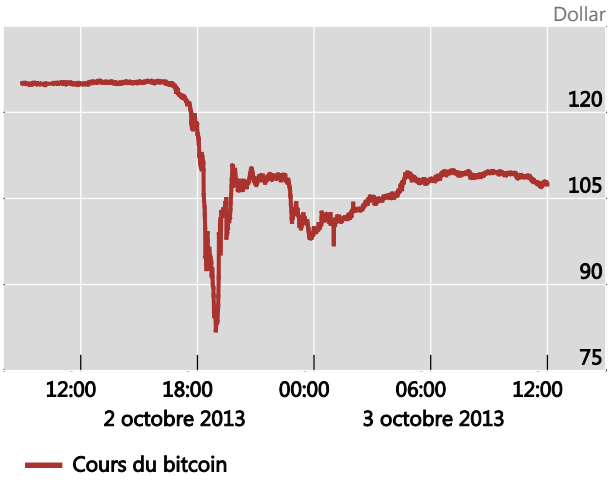
L'essor des cryptomonnaies et de la technologie qui leur est associée soulève un certain nombre de questions en termes de politiques publiques. Les autorités cherchent des moyens d'assurer l'intégrité des marchés et des systèmes de paiement, de protéger consommateurs et investisseurs, et de préserver la stabilité financière globale. En la matière, la lutte contre l'utilisation illicite de fonds constitue un défi de taille. Dans le même temps, les autorités veulent maintenir les incitations de long terme à l'innovation, et notamment le principe « même risque, même régulation »[29]. S'il s'agit là pour l'essentiel d'objectifs courants, les cryptomonnaies créent aussi de nouveaux enjeux, et pourraient nécessiter de nouveaux outils et de nouvelles approches. Se pose également la question de savoir si les banques centrales devraient émettre leurs propres monnaies numériques (*central bank digital currency*, CBDC).

Défis réglementaires

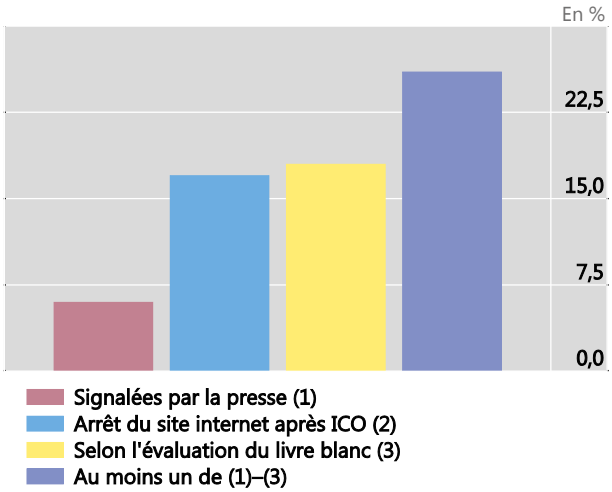
Un premier enjeu réglementaire clé est la lutte contre le blanchiment d'argent et le financement du terrorisme. La question est de savoir si, et à quel point, l'essor des cryptomonnaies a ouvert une brèche dans cette lutte en permettant le contournement de mesures telles que les règles relatives à la connaissance des clients. L'utilisation des cryptomonnaies étant fondée sur l'anonymat, il est difficile de déterminer dans quelle mesure elles servent à contourner les contrôles des capitaux et le fisc, ou à financer des transactions illégales. Néanmoins, des exemples comme la forte réaction du marché du Bitcoin à la fermeture de Silk Road – plateforme majeure de vente et d'achat de drogues – semblent montrer qu'une part non négligeable de la demande de cryptomonnaies est liée à des activités illicites (graphique V.9, cadre de gauche)[30].

Fermeture d'une plateforme d'échanges illégale et légitimité des ICO — Graphique V.9

Réaction du cours du Bitcoin à la fermeture de la plateforme Silk Road[1]



Une grande partie des ICO seraient frauduleuses



[1] Prix du bitcoin lors de la fermeture de Silk Road en octobre 2013.

Sources : Boslego, J., Catalini, C., et Zhang, K., « Technological opportunity, bubbles and innovation: the dynamics of initial coin offerings », *MIT Working Papers*, à paraître ; CoinDesk.

Un autre défi réglementaire a trait aux règles relatives aux valeurs mobilières et autres réglementations visant à protéger les consommateurs et les investisseurs. Un problème commun est le vol sur internet. Compte tenu de la taille et de la lourdeur des registres distribués, ainsi que des coûts de transactions élevés, la plupart des utilisateurs accèdent à leurs avoirs en cryptomonnaies par l'intermédiaire de tierces parties telles que les « fournisseurs de portefeuilles de cryptomonnaies » ou les « plateformes d'échange de cryptomonnaies ». Paradoxalement – et contrairement à la promesse initiale du Bitcoin et d'autres cryptomonnaies –, de nombreux utilisateurs qui s'étaient tournés vers les cryptomonnaies par défiance envers les banques et l'État ont fini par recourir à des intermédiaires non réglementés. Certains de ceux-ci (comme Mt Gox ou Bitfinex) se sont avérés frauduleux, ou ont eux-mêmes été victimes de piratage[31].

La fraude est également endémique dans le domaine des « initial coin offerings » (ICO). Ce type de levée de fonds consiste à proposer au public une certaine quantité d'unités de cryptomonnaies, le produit de l'émission conférant parfois des droits de participation dans une start-up. Malgré les avertissements lancés par les autorités, les investisseurs se sont massés sur les ICO, bien que celles-ci soit souvent liées à des projets commerciaux opaques, faisant l'objet d'informations très limitées et non auditées. Nombre de ces projets se sont révélés être des pyramides de Ponzi (graphique V.9, cadre de droite).

Un troisième défi réglementaire concerne, à plus long terme, la stabilité du système financier. La possibilité qu'un large recours aux cryptomonnaies et aux produits financiers à exécution automatique qui leur sont liés donne naissance à de nouvelles fragilités financières et à de nouveaux risques systémiques nécessite un suivi étroit de l'évolution de ces marchés. Compte tenu de leurs profils de risque singuliers, ces technologies requièrent un renforcement des ressources à la disposition des autorités de régulation et de contrôle. Dans certains cas, comme l'exécution d'importants volumes de paiements à valeur élevée, le périmètre réglementaire pourrait devoir être étendu aux entités utilisant les nouvelles technologies, afin d'éviter l'accumulation de risques systémiques.

La nécessité de renforcer les réglementations ou d'en établir de nouvelles et de surveiller les cryptomonnaies et les crypto-actifs ne fait guère débat au sein des autorités de régulation du monde entier. Dans un récent communiqué, le G20 des ministres des finances et gouverneurs de banque centrale a notamment évoqué la protection des consommateurs et des investisseurs, l'intégrité du marché, la fraude fiscale, le blanchiment d'argent et le financement du terrorisme, et a appelé les instances de normalisation internationales à poursuivre le suivi de ces questions. Il a également souhaité que le Groupe d'action financière internationale progresse dans la mise en œuvre des normes applicables à l'échelle mondiale[32].

La conception et la mise en œuvre effective de normes renforcées sont toutefois difficiles. Les définitions juridiques et réglementaires ne correspondent pas toujours aux nouvelles réalités. Les technologies sont utilisées dans de multiples activités économiques, qui dans bien des cas sont régulées par des autorités différentes. Ainsi, les ICO sont actuellement utilisées par des entreprises de technologie pour lever des fonds en vue de projets n'ayant rien à voir avec les cryptomonnaies. Au-delà de la terminologie – les ICO consistant à émettre des unités de cryptomonnaies tandis que les IPO (appels publics à l'épargne classiques) se traduisent par l'émission d'actions – les premières ne diffèrent guère des secondes sur des plateformes d'échanges établies ; il serait donc naturel que les autorités boursières leur appliquent les mêmes mesures de régulation et de surveillance. Certaines ICO ont cependant vocation à

donner accès à de futurs logiciels, dans les jeux vidéo par exemple, au moyen de « jetons d'utilité ». Il ne s'agit alors pas d'une activité d'investissement et ces opérations devraient relever des lois sur la protection des consommateurs et des autorités qui en sont chargées[33].

Au plan opérationnel, le principal facteur de complication tient au fait que les cryptomonnaies sans autorisation attribuée ne trouvent pas facilement leur place dans les dispositifs existants. Il leur manque notamment une personne morale susceptible de s'inscrire dans le périmètre réglementaire. Les cryptomonnaies évoluent dans leur propre monde numérique, sans frontières, et peuvent en grande partie fonctionner indépendamment des environnements institutionnels existants ou de toute autre infrastructure. Leur domicile légal – si tant est qu'elles en aient un – peut être extraterritorial, ou impossible à établir de manière claire. En conséquence, elles ne peuvent faire l'objet que d'une réglementation indirecte.

Quel type d'approche réglementaire les autorités peuvent-elles suivre ? Trois éléments doivent être pris en compte.

D'abord, l'essor des cryptomonnaies et des crypto-actifs appelle une redéfinition du périmètre réglementaire. Celui-ci doit inclure une nouvelle réalité où les lignes de démarcation des responsabilités des différents régulateurs entre et au sein des juridictions sont de plus en plus floues[34]. Les cryptomonnaies étant par nature internationales, seul un effort coordonné de régulation à l'échelle mondiale a une chance d'être efficace[35].

Ensuite, l'interopérabilité des cryptomonnaies avec les entités financières réglementées pourrait être prise en considération. Seules des plateformes d'échanges réglementées peuvent fournir la liquidité nécessaire aux produits financiers fondés sur la DLT pour dépasser le simple marché de niche, et les flux de règlement doivent en définitive être convertis en monnaie souveraine. Les règles en termes d'impôt et de traitement des fonds propres applicables aux établissements réglementés souhaitant réaliser des transactions en actifs liés à des cryptomonnaies pourraient donc être adaptées. Les régulateurs pourraient surveiller si, et de quelle manière, les banques émettent ou reçoivent des cryptomonnaies en guise de sûreté.

Enfin, la réglementation peut cibler les établissements offrant des services propres aux cryptomonnaies. Ainsi, pour mener une lutte efficace contre le blanchiment d'argent et/ou le financement du terrorisme, les régulateurs pourraient concentrer leurs efforts sur le moment précis où une cryptomonnaie est convertie en monnaie souveraine. D'autres lois et réglementations existantes relatives aux services de paiement portent sur les questions de sécurité, d'efficacité et de légalité d'utilisation. Ces principes pourraient aussi s'appliquer aux fournisseurs d'infrastructures de cryptomonnaie, tels que les « portefeuilles de cryptomonnaie »[36]. Pour éviter toute brèche, la réglementation devrait, dans l'idéal, être largement comparable, et mise en œuvre de manière homogène, à travers les juridictions.

Les banques centrales devraient-elles émettre des monnaies numériques ?

Une question de politique publique concerne, à moyen terme, l'émission de monnaies numériques par les banques centrales (*central bank digital currency*, CBDC), ainsi que le public auquel s'adresseraient ces monnaies le cas échéant. Les CBDC fonctionneraient à la manière des espèces : les banques centrales commenceraient par émettre des CBDC qui circuleraient ensuite entre les banques, les entreprises non

financières et les consommateurs, sans intervention supplémentaire de la banque centrale[37]. Une CBDC de ce type pourrait être échangée de manière bilatérale entre acteurs du secteur privé à l'aide de registres distribués sans que la banque centrale ait à en assurer le suivi et actualiser les soldes. Elle serait fondée sur un registre distribué à autorisation attribuée (graphique V.2), la banque centrale déterminant qui agit en tant que nœud de confiance.

Si la distinction entre une CBDC d'usage général et les passifs numériques existants de banque centrale (solde des réserves des banques commerciales) peut sembler technique, elle est en réalité fondamentale quant aux implications pour le système financier. Une CBDC d'usage général, émise à destination des ménages et des entreprises, pourrait profondément affecter trois domaines au cœur de l'activité des banques centrales : les paiements, la stabilité financière et la politique monétaire. Un récent rapport conjoint du Comité sur les paiements et les infrastructures de marché et du Comité des marchés souligne les enjeux sous-jacents[38]. Les auteurs concluent que les forces et les faiblesses d'une CBDC d'usage général dépendraient de la manière dont elle serait conçue. Ils notent aussi que, si aucun candidat majeur à l'émission d'une telle monnaie n'est pour l'instant apparu, un instrument de ce type présenterait d'importantes fragilités, les bénéfices étant en revanche moins clairs.

À ce stade, les banques centrales suivent attentivement l'évolution de ces technologies tout en conservant une approche prudente en termes de mise en application. Certaines d'entre elles évaluent les avantages et les inconvénients de l'émission de CBDC beaucoup plus ciblées, limitées aux transactions de gros entre établissements financiers. Ces CBDC ne remettraient pas en question l'actuel système à deux niveaux ; elles viseraient plutôt à renforcer l'efficacité opérationnelle des mécanismes existants. Pour l'instant néanmoins, les expériences menées sur de telles CBDC de gros ne plaident pas fortement en faveur d'une émission de ce type de monnaie à court terme (encadré V.C).

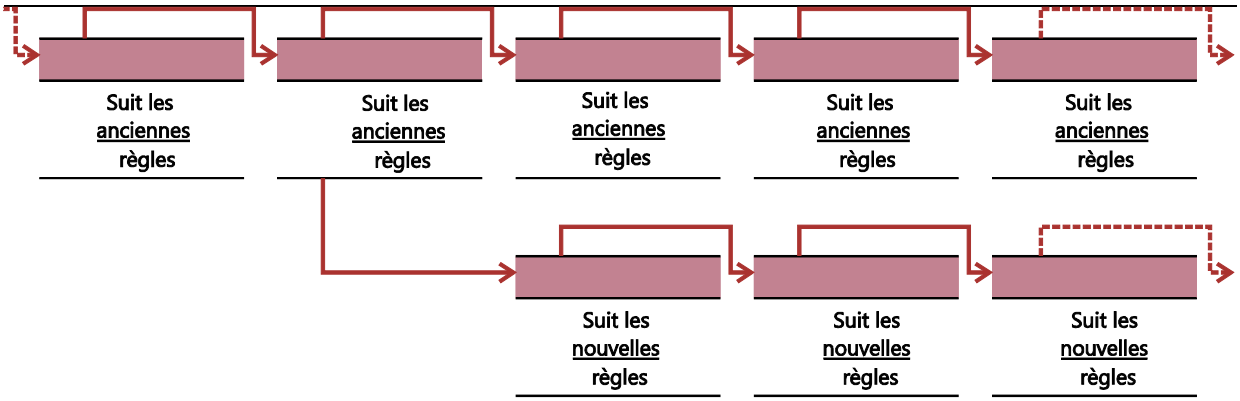
Encadré V.A

Le phénomène de bifurcation et l'instabilité du consensus décentralisé dans la chaîne de blocs

Le phénomène de bifurcation, ou « forking » en anglais, a contribué à l'augmentation rapide du nombre de cryptomonnaies (graphique V.6, cadre de droite). Ainsi, le mois de janvier 2018 a vu à lui seul l'apparition des sous-branches du Bitcoin que sont Bitcoin ALL, Bitcoin Cash Plus, Bitcoin Smart, Bitcoin Interest, Quantum Bitcoin, Bitcoin Lite, Bitcoin Ore, Bitcoin Private, Bitcoin Atom et Bitcoin Pizza. Les modalités de création de ces sous-branches sont diverses et les sous-branches elles-mêmes peuvent être temporaires ou permanentes. Prenons l'exemple des bifurcations non rétrocompatibles, ou « hard fork » en anglais (graphique V.A). Ce phénomène se produit si certains mineurs d'une cryptomonnaies se concertent pour changer le protocole au profit d'une nouvelle série de règles incompatibles avec les anciennes règles. Ces modifications peuvent affecter de nombreux aspects du protocole, tels que la taille maximale autorisée des blocs, la fréquence à laquelle des blocs peuvent être intégrés à la chaîne de blocs, ou un changement de la preuve de transaction requise pour actualiser cette chaîne. Les mineurs qui adoptent les nouvelles règles partent de la chaîne de bloc originale et lui ajoutent ensuite des blocs qui ne sont pas reconnus par les mineurs qui continuent de suivre les anciennes règles. Ceux-ci continuent de développer la chaîne de bloc initiale. Ainsi, deux chaînes séparées se développent en parallèle, chacune ayant son propre historique de transactions.

Exemple de bifurcation non rétrocompatible

Graphique V.A



Source : BRI.

De fréquents épisodes de « forking » peuvent être révélateurs d'un problème spécifique aux modalités de formation du consensus dans le réseau décentralisé de mineurs d'une cryptomonnaie. Le problème économique sous-jacent est que ce consensus décentralisé n'est pas unique. La règle consistant à suivre la chaîne la plus longue incite les mineurs à suivre la majorité de la communauté de calcul mais ne détermine pas une trajectoire unique pour la majorité elle-même. Par exemple, si un mineur pense que la toute dernière mise à jour du registre sera ignorée par le reste du réseau de mineurs, il a lui-même intérêt à ignorer cette mise à jour. Et si la majorité des mineurs décide d'ignorer une mise à jour, ils créent de fait un nouvel équilibre. Des équilibres aléatoires peuvent ainsi voir le jour – et ont effectivement déjà vu le jour, comme en témoignent le phénomène de « forking » et l'existence de milliers de blocs « orphelins » (dans le cas du Bitcoin) ou « oncles » (pour l'Ether) qui ont été rétroactivement invalidés. Il existe d'autres inquiétudes à l'égard de la fiabilité de l'actualisation décentralisée de la chaîne de blocs, qui tiennent au fait que les mineurs sont incités à réaliser une bifurcation stratégique dès que le dernier bloc ajouté par un autre mineur entraîne des frais de transaction élevés, qui peuvent être détournés par l'invalidation dudit bloc sous l'effet d'une bifurcation①.

① Pour une analyse de la singularité du processus d'actualisation de la chaîne de blocs, voir Biais, B., Bisière, C., Bouvard M. et Casamatta C. (2017), « The blockchain folk theorem », *TSE Working Paper* n° 17-817. Pour une analyse des motifs stratégiques présidant à la création d'une bifurcation, voir Carlsten, M., Kalodner, H., Weinberg, S.M., Narayanan, A. (2016), « On the instability of bitcoin without the block reward », *Compte-rendu de la Conférence 2016 ACM SIGSAC sur la sécurité informatique et des communications*.

Encadré V.B

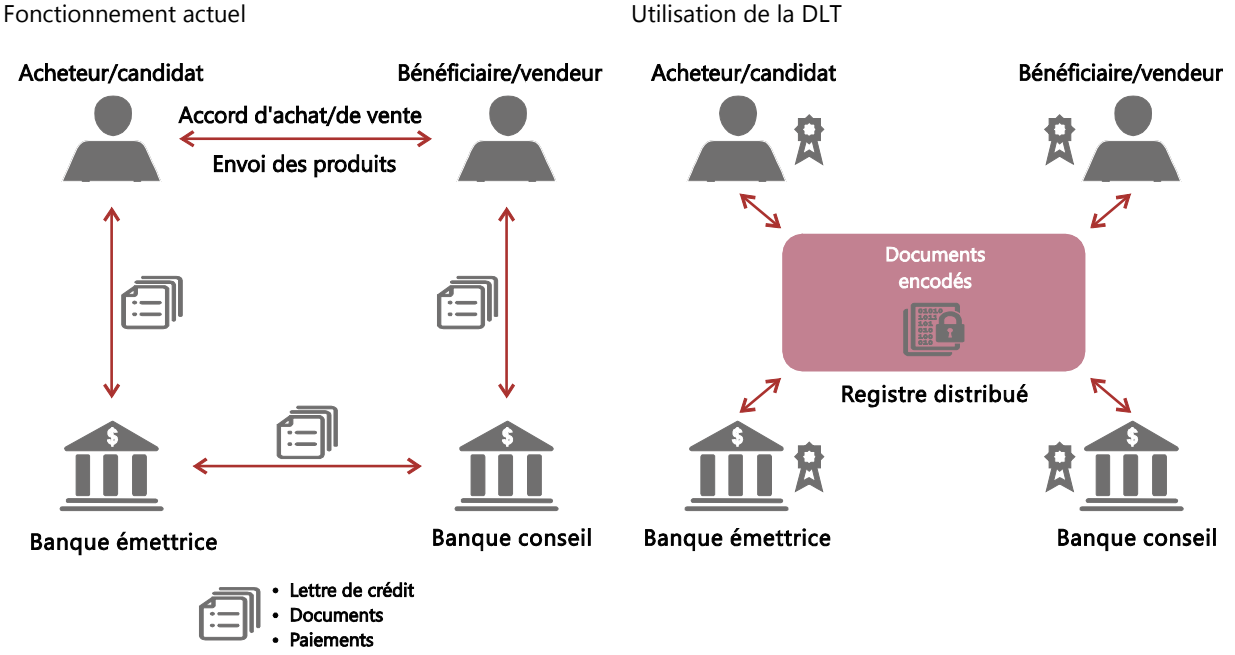
La technologie du registre distribué dans le crédit commercial

Selon l'Organisation mondiale du commerce, 80 à 90 % des échanges mondiaux s'appuient sur le crédit commercial. Lorsqu'un exportateur et un importateur s'accordent sur un échange, l'exportateur préfère souvent être réglé à l'avance afin d'éviter le risque d'impayé. De son côté, l'importateur souhaite réduire ses propres risques et requiert des documents prouvant que les biens ont effectivement été envoyés avant de donner l'ordre de paiement.

Les solutions de crédit commercial offertes par les banques et autres établissements financiers visent à assurer le relais entre exportateurs et importateurs. Le plus souvent, une banque implantée dans le pays d'origine de l'importateur émet une lettre de crédit garantissant le paiement à l'exportateur à la réception de la preuve d'envoi (de type connaissement) des marchandises. Dans le pays de l'exportateur, une banque peut faire crédit à ce dernier en échange de cette garantie, et collecter le paiement auprès de la banque de l'importateur afin de finaliser la transaction.

Dans sa forme actuelle (graphique V.B, cadre de gauche), le crédit commercial constitue une démarche fastidieuse, coûteuse et complexe. Il nécessite de multiples échanges de documents entre l'exportateur, l'importateur, leurs banques respectives et les agents effectuant les contrôles physiques des marchandises envoyées à chaque point de passage, ainsi qu'avec les services des douanes, les agences publiques de crédit à l'exportation ou les assureurs de fret. Il s'agit donc souvent d'un processus bureaucratique, que la technologie DLT peut simplifier en accélérant l'exécution des contrats sous-jacents. Ainsi, un contrat intelligent (« smart contract ») peut automatiquement ordonner le paiement à l'exportateur une fois qu'un connaissement a été dûment intégré au registre. En outre, une meilleure disponibilité des informations concernant les envois de marchandises déjà financés pourrait réduire le risque de voir des exportateurs obtenir illégalement de multiples crédits auprès de différentes banques pour le même envoi.

Modalités de fonctionnement du crédit commercial à l'aide d'un registre distribué — Graphique V.B



Source : adapté de www.virtusapolaris.com.

Encadré V.C

Les monnaies numériques de banque centrale

Au cours des dernières décennies, les banques centrales ont exploité les nouvelles technologies numériques pour améliorer l'efficacité et la solidité des paiements et du système financier dans son ensemble. Ces technologies ont permis aux banques centrales de réaliser des économies dans l'apport de liquidité aux systèmes de règlement brut en temps réel (*Real Time Gross Settlements,* RTGS). En associant ces dispositifs au système de règlement en continu (*Continuous Linked Settlement*, CLS), les banques commerciales du monde entier procèdent chaque jour, en permanence, au règlement de milliers de milliards de dollars de transactions en devises. Le CLS permet de supprimer le « risque Herstatt » qui, auparavant, menaçait sensiblement la stabilité financière– le risque qu'une banque correspondante intervenant dans le cadre d'une opération de change rencontre des difficultés financières avant d'avoir payé l'équivalent en devises au destinataire désigné. Plus récemment, des systèmes plus rapides de paiement de détail se sont développés dans le monde entier et les banques centrales promeuvent et facilitent activement cette tendance.

Dans le cadre d'initiatives de plus grande ampleur dans les nouvelles technologies de paiement, les banques centrales expérimentent aussi des CBDC de gros. Il s'agit d'une nouvelle version, fondée sur des jetons, des traditionnels comptes de réserve et de règlement. L'intérêt de CBDC de gros fondées sur la DLT dépend de la capacité de ces technologies à améliorer l'efficacité et à réduire les coûts d'exploitation et de règlement. Les bénéfices pourraient être substantiels, dans la mesure où de nombreux systèmes actuels de paiements de gros gérés par les banques centrales font appel à des technologies dépassées et coûteuses à entretenir.

La mise en œuvre de CBDC de gros soulève deux principaux défis. D'abord, les limites de la DLT sans autorisation attribuée s'appliquent aussi aux CBDC de gros, ce qui signifie que celles-ci doivent être conçues sur des modèles recourant aux protocoles à autorisation attribuée. Ensuite, les choix effectués en termes de modalités de conversion des réserves des banques centrales vers et à partir du registre distribué doivent être prudents, de façon à préserver la liquidité intrajournalière tout en minimisant les risques de règlement.

Un certain nombre de banques centrales, y compris l'Autorité monétaire de Singapour (projet Ubin), la Banque du Canada (projet Jasper), la Banque centrale européenne et la Banque du Japon (projet Stella) ont déjà expérimenté l'exploitation de systèmes RTGS de gros pour des CBDC fondées sur la DLT. Dans la plupart des cas, les banques centrales ont choisi une approche de dépôt numérique, dans laquelle elles émettent des jetons numériques sur un registre distribué, adossés à, et remboursables dans, leurs réserves détenues sur un compte séparé. Les jetons peuvent ensuite servir à des transferts interbancaires sur un registre distribué.

Les banques centrales publient actuellement les résultats de leurs expériences. Au stade initial, chacune de celles-ci a largement réussi à reproduire les systèmes de paiement de gros existants. Cependant, ces résultats ne se sont pas révélés clairement supérieurs aux infrastructures existantes①.

① Voir Bech, M. et Garratt, R. (2017), « Des cryptomonnaies émises par les banques centrales ? », *Rapport trimestriel BRI*, septembre, et CPIM et CM (2018), *Central bank digital currrencies*, mars.

Notes

[1] Dans ce domaine, la terminologie est fluctuante et continue d'évoluer, avec ce que cela comporte d'ambiguïtés juridiques et réglementaires. Dans le présent chapitre, l'utilisation du terme « cryptomonnaie » ne vise pas à formuler un point de vue particulier sur ce que sont les systèmes de protocole sous-jacents ; généralement, ces monnaies partagent certaines, mais pas l'ensemble, des caractéristiques d'une monnaie souveraine, et leur traitement juridique varie selon les juridictions. Dans certains cas, le chapitre prend pour exemple certaines cryptomonnaies ou certains crypto-actifs. Ces exemples ne sont pas exhaustifs et ne signalent en aucun cas une adhésion de la BRI ou de ses actionnaires à une cryptomonnaie, une entreprise, un produit ou un service en particulier.

[2] À ce sujet, voir également Carstens (2018a, c).

[3] Graeber (2011) avance que l'usage de la monnaie ne s'est vraiment répandu qu'avec l'invention des pièces, qui sont apparues en Chine, en Inde et en Lydie presque simultanément, vers 600-500 avant J.C. Il montre aussi que, contrairement à une idée courante, avant que la monnaie n'apparaisse, les échanges s'effectuaient essentiellement à l'aide de reconnaissances de dette mutuelles plutôt que par le troc.

[4] L'étude de ces fonctions a fait l'objet d'une abondante littérature. En voici quelques exemples clés : Kiyotaki et Wright (1989) montrent en quoi la monnaie utilisée comme moyen d'échange peut constituer un progrès par rapport au troc. Kocherlakota (1996) explique que lorsque la tenue parfaite d'un registre et des engagements n'est pas possible, la monnaie fait office de « mémoire » et permet de meilleurs résultats. Samuelson (1958) montre dans un modèle à générations imbriquées que la monnaie peut permettre des gains d'efficacité lorsqu'elle sert de réserve de valeur. Doepke and Schneider (2017) expliquent en quoi l'utilisation d'une unité de compte commune constitue une amélioration et pourquoi la monnaie d'un État constitue à la fois une unité de compte et un moyen d'échange.

[5] Citons par exemple les coquillages en Afrique, les fèves de coco chez les Aztèques et le wampum chez les Amérindiens. Même dans ces cas, il ne fait aucun doute que des relations de crédit coexistaient avec les mécanismes en place. Voir par exemple Melitz (1974) pour une analyse plus détaillée.

[6] Sur l'évolution des lettres de crédit et le rôle charnière qu'elles ont joué dans le développement des systèmes monétaires en général et dans le financement commercial en particulier, voir De Roover (1948, 1953). Pour une analyse historique et détaillée, voir Kindleberger (1984), qui propose une approche générale, et Santarosa (2015), qui étudie l'importance de l'introduction de la responsabilité conjointe.

[7] Une monnaie d'Etat adossée à un produit de base, comme l'étalon-or, a constitué une autre tentative de parvenir à un équilibre. Assurant une stabilité en temps normal, les contraintes dont il s'accompagne ont eu tendance à limiter la capacité des banques centrales à ajuster l'offre de monnaie en période de tensions économiques et financières. Dans des cas extrêmes, ces contraintes ont simplement été abandonnées et la monnaie est devenue inconvertible. Par exemple, à l'époque de l'étalon-or, la fonction de convertibilité de la monnaie en or pouvait être considérée comme un moyen d'empêcher l'émetteur souverain d'émettre des quantités excessives de monnaie et de dévaluer celle-ci. Cette contrainte était crédible en ce sens, précisément, que l'or a une valeur de marché indépendante de son utilisation en tant que monnaie, c'est-à-dire moyen de paiement. C'était une manière d'empêcher l'émetteur souverain de rendre les détenteurs de monnaie otages de son monopole d'émission. Pour une discussion plus poussée, voir Giannini (2011).

[8] Voir les travaux récents de Schnabel and Shin (2018), qui incluent l'analyse des incitations à la dévaluation de la monnaie.

[9] Voir Van Dillen (1964), Roberds and Velde (2014) et Bindseil (2018). Le lien avec les banques centrales est étudié par Ugolini (2017), Bindseil (2018) et Schnabel et Shin (2018).

[10] En outre, les banques centrales ont généralement eu la possibilité d'agir en tant que prêteur en dernier ressort. La récente Grande crise financière a de nouveau rappelé la fragilité comme la capacité d'adaptation des mécanismes monétaires existants, y compris dans les économies les plus avancées. Si la crise a mis en lumière les lacunes du dispositif réglementaire en vigueur, l'importance accrue accordée après la crise à la surveillance et à la régulation bancaires souligne la manière dont les mécanismes institutionnels peuvent évoluer dans le but d'entretenir la confiance dans la monnaie au sein du dispositif à deux niveaux.

[11] Voir Carstens (2018a). Giannini (2011) souligne aussi l'importance des mécanismes institutionnels régissant l'offre de monnaie : « L'évolution des institutions monétaires paraît être avant tout le fruit d'un dialogue continuel entre les sphères économiques et politiques qui, chacune à son tour,

produisent des innovations monétaires (...) et préservent l'intérêt général des abus résultant d'intérêts partisans. »

[12] De fait, les banques centrales supervisent aujourd'hui les systèmes de paiement et fournissent de grandes quantités de crédit intrajournalier pour parvenir à cette fin, notamment dans les systèmes de paiement de gros. En fonction des spécificités des mécanismes, ce crédit peut aussi être fourni d'un jour sur l'autre, ou à des échéances plus longues encore. Pour de plus amples précisions quant à ces mécanismes et aux procédures opérationnelles, entre autres, voir BRI (1994) et Borio (1997).

[13] Voir Bech and Garratt (2017) et CPIM-CM (2018) pour de plus amples précisions.

[14] À l'instar des billets de banque et autres jetons physiques, chaque transaction est vérifiée au regard de la preuve de paiement, c'est à-dire l'entrée qui lui est associée dans le registre. Cela diffère d'autres formes de monnaie électronique, où la vérification se fonde sur l'identité du titulaire du compte. Les cryptomonnaies sont donc des monnaies numériques basées sur des jetons.

[15] Parmi les exemples actuels ou à venir de cryptomonnaies recourant à un modèle à autorisation attribuée fondé sur des nœuds de confiance désignés figurent, entre autres, la monnaie numérique de la Fondation SAGA, Ripple, ainsi que le projet Utility Settlement Coin.

[16] Nous utilisons le terme « Bitcoin » pour désigner le protocole et le réseau d'utilisateurs et de mineurs de la cryptomonnaie, et « bitcoin » en référence à l'unité de compte.

[17] Ethereum, Litecoin et Namecoin en sont des exemples.

[18] Auer (2018) propose une description détaillée des composantes technologiques du Bitcoin et d'autres cryptomonnaies fondées sur la chaîne de blocs, telles que les signatures numériques, le hachage et l'enchaînement cryptographique des blocs. Voir aussi Berentsen and Schär (2018).

[19] Techniquement, cela passe par des fonctions de hachage cryptographique (telle que la fonction SHA(256) dans le cas du Bitcoin). Celles-ci ont pour spécificité de générer des résultats imprévisibles, de sorte qu'un résultat en particulier ne peut être produit que par tâtonnement.

[20] Pour qu'une cryptomonnaie sans autorisation attribuée fonctionne dans un environnement sans autorité garante de la confiance, tous les mineurs et utilisateurs doivent conserver un exemplaire actualisé de l'ensemble du registre. Il convient de noter cependant qu'en pratique, de nombreux utilisateurs se fient aux informations fournies par d'autres. Certains ne vérifient que le résumé d'informations relatif au registre au travers du processus nommé « vérification de paiement simplifiée ». Et à la grande différence de l'idée à l'origine du Bitcoin, un nombre plus important encore d'utilisateurs n'ont accès à leurs fonds qu'au travers du site internet d'une tierce partie. En pareil cas, la tierce partie seule contrôle les avoirs en cryptomonnaie de ses clients.

[21] Voir Nakamoto (2009), p. 8.

[22] Ceci passe par l'auto-calibrage des preuves de transaction, qui accroît le niveau nécessaire de difficulté mathématique au point que la puissance de calcul combinée de tous les mineurs suffit à peine à actualiser le registre au rythme fixé par le protocole.

[23] Voir Carstens (2018a).

[24] Si le problème de saturation pourrait être résolu en autorisant une augmentation de la taille des blocs, cette solution pourrait en réalité s'avérer encore plus néfaste. Au-delà de la rémunération des blocs, une certaine saturation est nécessaire pour inciter les utilisateurs à payer le traitement de leurs transactions, car si le système fonctionne à un niveau inférieur à sa limite, toutes les transactions seront traitées et les utilisateurs rationnels ne verseront que de très faibles frais de transaction. Les mineurs n'auraient aucun intérêt à participer à l'actualisation des transactions et l'équilibre du système pourrait s'effondrer. Voir par exemple Hubermann et al. (2017) et Easly et al. (2017), ainsi que Abadi et Brunnermeier (2018).

[25] En termes techniques, l'interaction entre les utilisateurs est celle de substituts stratégiques et non pas de compléments stratégiques. Les cryptomonnaies sont donc moins un jeu de coordination qu'un jeu de congestion.

[26] La nature probabiliste de l'irrévocabilité pourrait notamment aboutir à une accumulation des risques si les cryptomonnaies étaient utilisées dans des systèmes de gros, où les fonds tendent à être réinvestis sans délai. Une telle utilisation créerait en fait une dimension entièrement nouvelle de risque global, la probabilité que l'historique des transactions dans son ensemble ne soit pas irrévocable affectant toutes les expositions.

[27] Les propositions ne manquent pas en la matière, mais la plupart n'ont pas encore été éprouvées. Les protocoles de cryptomonnaies pourraient se passer du système coûteux de preuves de transaction en le remplaçant par un système de « preuve de participation », l'idée étant d'assurer la crédibilité

du dispositif en mettant en jeu les avoirs en cryptomonnaies plutôt qu'en procédant à d'onéreux calculs informatiques. Parmi les solutions proposées pour résoudre le problème d'extensibilité figure Lightning Network, qui déplace les petites transactions de la chaîne de blocs principale vers un environnement séparé pré-capitalisé. Il existe aussi de nouvelles cryptomonnaies, comme IOTA, qui visent à remplacer la chaîne de blocs par un registre et une structure de vérification plus complexes.

[28] Voir Juskalian (2018).

[29] Voir Carstens (2018a).

[30] Les représentants de l'État ne semblent pas non plus insensibles à l'attrait des cryptomonnaies : deux agents de l'administration américaine ont ainsi été accusés de vol de bitcoins qui avaient été saisis lors de la fermeture de Silk Road.

[31] Par exemple, la plupart des paiements en bitcoin réalisés au moyen d'un smartphone ces derniers temps est très probablement passé par une tierce partie, étant donné que la taille actuelle de la chaîne de blocs dépasse la capacité de stockage de la plupart de ces téléphones. Reuters (2017) et Moore et Christin (2013) répertorient certains cas dans lesquels ces tierces parties se sont révélées frauduleuses ou ont été victimes de piratage. Pour une analyse des utilisations illicites des cryptomonnaies, voir Fanusie et Robinson (2018) et Foley et al. (2018).

[32] Voir G20 des ministres des finances et gouverneurs de banque centrale (2018).

[33] Concernant la réglementation des ICO par opposition aux IPO, et dans une perspective américaine, Clayton (2017) estime qu' « une évolution de la structure d'une offre de titres n'affecte pas le principe fondamental selon lequel une offre de valeurs mobilières doit entraîner l'application de la législation sur les valeurs mobilières. » En Suisse, la FINMA (2018) a établi un dispositif réglementaire qui classe les ICO selon l'utilisation finale des jetons (jetons de paiement, jetons d'investissement ou jetons d'utilité).

[34] Techniquement, pour que les cryptomonnaies fondées sur un protocole puissent fonctionner, il suffit qu'un pays au moins y permette l'accès. Les problèmes rencontrés par les autorités pour fermer des sites de téléchargement illégal tels que Napster ou The Pirate Bay et les protocoles de téléchargement comme BitTorrent montrent à quel point le respect des règles peut être difficile à assurer.

[35] Le Groupe d'action financière internationale (2015) affirme qu'il est essentiel que les différentes juridictions traitent de la même manière les produits et services similaires selon leurs fonctions et profils de risque pour améliorer l'efficacité des normes internationales contre le blanchiment d'argent.

[36] Un problème tient au fait que les paiements sont réglementés par des autorités et des législations aux objectifs très hétérogènes (surveillance des systèmes de paiement, contrôle prudentiel, protection des consommateurs, lutte contre le financement du terrorisme et lutte contre le blanchiment d'argent). Par exemple, les établissements basés aux États-Unis doivent entre autres se conformer à la loi sur le secret bancaire, au Patriot Act et aux réglementations du Bureau de contrôle des actifs étrangers. Par ailleurs, l'applicabilité de la législation existante aux nouveaux instruments ne va pas de soi. Ainsi, dans l'Union européenne, la définition juridique de la monnaie électronique inclut l'obligation selon laquelle les soldes doivent représenter une créance sur l'émetteur. Comme les cryptomonnaies ne constituent aucune créance, elles ne peuvent pas être considérées comme des monnaies électroniques et ne sont donc, par défaut, pas couvertes par la législation en question.

[37] La mise en œuvre de CBDC fondées sur des jetons pourrait prendre différentes formes. Ces CBDC pourraient s'appuyer sur la DLT et présenter les mêmes caractéristiques que les cryptomonnaies, à ceci près que la banque centrale, plutôt que le protocole lui-même, contrôlerait les montants émis et garantirait la valeur du jeton.

[38] CPIM-CM (2018).

Références

Abadi, J. et Brunnermeier, M. (2018), « Blockchain economics », Princeton University, mai, non publié.

Auer, R. (2018), « The mechanics of decentralised trust in Bitcoin and the blockchain » *BIS working papers*, à paraître.

Autorité fédérale de surveillance des marchés financiers (FINMA) (2018), Guide pratique pour les questions d'assujettissement concernant les initial coin offerings (ICO), 16 février.

Banque des Règlements Internationaux (1994), *64ème Rapport annuel*, juin.

Bech, M., et Garratt, R. (2017), « Des cryptomonnaies émises par les banques centrales ? », *Rapport trimestriel BRI*, septembre 2017, p. 55-70

Berentsen, A. et Schär, F. (2018), « A short introduction to the world of cryptocurrencies », Federal Reserve Bank of St. Louis, *Review*, vol. 100, n° 1.

Blindseil, U. (2018), « Pre-1800 central bank operations and the origins of central banking », Université de Mannheim, non publié.

Borio, C. (1997), « The implementation of monetary policy in industrial countries: a survey », *BIS Economic Papers,* n° 47, juillet.

Carstens, A. (2018a), « Money in the digital age: what role for central banks? », discours prononcé à la House of Finance de l'Univeristé Goethe, Francfort, le 6 février.

——— (2018b), « Central Banks and cryptocurrencies: guarding trust in a digital age », intervention à la Brookings Institution, Washington, DC, 17 avril.

——— (2018c), « Technology is no substitute for trust », *tribune publiée dans Börsen-Zeitung*, 23 mai.

Catalini, C., Boslego, J. et Zhang, K. (2018), « Technological opportunity, bubbles and innovation: the dynamics of initial coin offerings », *MIT Working Papers*, à paraître.

Clayton, J. (2017), « Statement on cryptocurrencies and initial coin offerings », www.sec.gov/news/public-statement/statement-clayton-2017-12-11, 11 décembre.

Comité sur les paiements et les infrastructures de marché (2017), *Statistiques sur les systèmes de paiement, de compensation et de règlement dans les pays membres du CPIM*, décembre.

De Roover, R. (1948), « Money, banking and credit in mediaeval Bruges: Italian merchant-bankers Lombards and money changers, a study in the origins of banking », Mediaeval Academy of America.

——— (1953), *L'évolution de la lettre de change : XIVe-XVIIIe siècle*, Armand Colin.

Doepke, M. et Schneider, M. (2017), « Money as a unit of account », *Econometrica*, vol. 85, n° 5, pp. 1537-74.

Easley, D., O'Hara, M. et Basu, S. (2017), « From mining to markets: The evolution of Bitcoin transaction fees », papers.ssrn.com/sol3/papers.cfm?abstract_id=3055380.

Fanusie, Y. et Robinson, T. (2018), « Bitcoin laundering: an analysis of illicit flows into digital currency services », Center on Sanctions & Illicit Finance memorandum, janvier.

Foley, S., Karlsen, J.R. et Putniņš, T.J (2018), « Sex, drugs, and bitcoin: how much illegal activity is financed through cryptocurrencies? », dx.doi.org/10.2139/ssrn.3102645.

G20 des ministres des finances et gouverneurs de banque centrale (2018), communiqué publié à l'issue du Sommet de Buenos Aires, 19-20 mars.

Giannini, C. (2011), *The age of central banks*, Edward Elgar.

Graeber, D. (2011), *Debt: The first 5,000 years*, Melville House.

Groupe d'action financière international (2015), *Guidance for a risk-based approach to virtual currencies*, juin.

Huberman, G., Leshno, J. et Moellemi, C. (2017), « Monopoly without a monopolist: an economic analysis of the Bitcoin payment system », *Columbia Business School Research Paper*, n° 17-92.

Juskalian, R. (2018), « Inside the Jordan refugee camp that runs on blockchain », *MIT Technology Review*, édition en ligne, 12 avril.

Kindleberger, C. (1984), *A financial history of western Europe*, Allen & Unwin.

Kiyotaki, N. et Wright, R. (1989), « Money as a medium of exchange », J*ournal of Political Economy*, vol. 97, n° 4, pp. 927-54.

Kocherlakota, N. (1996), « Money is memory », *Journal of Economic Theory*, vol. 81, n° 2, pp. 232-51.

Melitz, J. (1974), *Primitive and modern money: an interdisciplinary approach*, Addison-Wesley.

Moore, T. et Christin, N. (2013), « Beware the middleman: empirical analysis of Bitcoin-exchange risk », in A-R Sadeghi (sous la direction de), *Lecture Notes in Computer Science*, vol. 7859.

Nakamoto, S. (2009), « Bitcoin: a peer-to-peer electronic cash system », *livre blanc*.

Reuters (2017), « Cryptocurrency exchanges are increasingly roiled by hackings and chaos », 29 septembre.

Roberds, W. et Velde, F. (2014), « Early public banks », *Federal Reserve Bank of Chicago Working Paper*, n° 2014-03.

Samuelson, P. (1958), « An exact consumption-loan model of interest with or without the social contrivance of money », *Journal of Political Economy*, vol. 66, n° 6, pp. 467-82.

Santarosa, V. (2015), « Financing long-distance trade: the joint liability rule and bills of exchange in eighteenth-century France », *The Journal of Economic History*, vol. 75, n° 3, pp. 690–719.

Schnabel, I. et Shin, H.S. (2018), « Money and trust: lessons from the 1620s for money in the digital age », *BIS Working Papers*, n° 698, février.

Ugolini, S. (2017), *The evolution of central banking: theory and history*, Palgrave-Macmillan.

Van Dillen, J.G. (1964), *History of the principal public banks*, Frank Cass & Co LTD.